Case Study

Cheating 2.0

How to Fight Back Against Cheaters

By Dave Meissner,

Vice President, Solution Services, Prometric

In today's world, it's almost impossible to find an adult who has not taken a test of some kind. From GCSE's, A Levels, University entrance exams and IT certification exams to corporate training, and even food handling – testing has likely played a part in the lives of every professional adult. In the case of licensing, the ability to work in a chosen profession hinges on a test result. For a professional certification, the ability to differentiate oneself as "a better option" or validate a skill set is dependent upon passing that exam. When you combine that with the reality that most adults would need to take precious time out of an already busy day to study for these exams on topics for which they may be ill-prepared or "rusty", you may come to find that some individuals are tempted to turn to cheating as the way forward. With "Technology 2.0" advances (including cell phone cameras, PDAs, iPods, microcomputers and computerized testing environments), it might seem that passing exams thanks to corrupt means would be easy.

Certification and licensing exams are a measure of qualification increasingly relied upon to gauge an individual's knowledge, skills and abilities. The results of these exams are used by managers for employment decisions and by government agencies and the general public when seeking qualified professionals. The value placed on testing has resulted in various threats to the security and validity of the process; a process which protects the public from those who are unqualified and/or seek credentials through fraudulent means. Particularly in tough economic times, when unemployment rates are soaring, picking up added skills can mean the difference between landing a job and being first runner up. And unfortunately, lying about those skills by either fudging resumes or cheating to pass the exams that identify someone as an expert can be tempting.

Desperate candidates might try anything to get ahead, from securing advance copies of an exam, or computing answers using handheld computers or high-feature cell phones to hiring someone else to impersonate them at the test centre. These advances in cheating technology, or Cheating 2.0, may seem insurmountable for certification verification, but test sponsors and test services providers are fighting back. Large-scale test administrators take proactive steps to ensure that advances in cheating never gain a foothold at their facilities. Whether crib sheets, PDAs or even false identities, these test services providers have tried and true ways to combat underhanded methods and offer a fair and secure testing environment that is truly reflective of a candidate's level of skill. In fact, as technology that can be used to cheat evolves – so too does the technology used to prevent it.

Security 101: The Basics of Prevention

Any test worth taking occurs in a proctored environment – either a bricks and mortar test centre run by a testing provider or a location at another type of a facility where proctors are brought in specifically for the testing event. When securing a test centre facility, first and foremost is maintaining **a safe and cheat-free testing environment**. Test centre operators have a waiting space along with a separate "testing room" to delineate the secure testing environment from the registration and intake area. Generally, nothing outside of the test candidate's physical body is allowed in the secure testing room, eliminating the possibility of using a device outside of one's brain to aid in the process. If any materials are allowed by the test sponsor, such as scratch paper, the test centre will provide its own to the candidate at the time of check-in to ensure that test takers are not able to "smuggle in" notes written down beforehand. Best practices often include the provision of colour-coded whiteboards or scratch paper, distributed at the beginning of a testing session and collected and counted at the end. This ensures that candidates not only don't smuggle notes into the exam – but ensures that they don't copy exam questions onto the note paper and smuggle them out, giving candidates who've not yet taken the exam an unfair advantage.

The identity of the candidate must also be assured. When a candidate arrives at a test centre they are asked to present either one or two valid, government issued IDs containing photo and signature. The identification is then swiped through a machine that reads the information stored in the magnetic strip or bar code on the back of the identification. This information is then compared against the "visible" information on the front of the ID(s) presented in order to ensure a match.

Inside the testing area, candidates are placed in workspaces that are partitioned off from others so that they cannot view their neighbours' exams. Test centre administrators and proctors patrol the testing area at specific intervals to look for abnormalities. For added security, many test centres use a **closed-circuit television** (CCTV) system to focus on candidates' faces and hands. If something out of the ordinary comes to light during the testing process, the test centre administrator can take a closer look by "zooming in." The footage can also be reviewed at a later time to determine exactly what happened during the course of the exam if an abnormality presents itself during scoring.

And who, exactly, does monitor what goes on in the exam room? Test Centre Administrators (TCAs) are the watchful professionals responsible for ensuring candidates are who they say they are, walking through the testing room at regular intervals to physically proctor the exams and guaranteeing that candidates are not able to sneak any materials into the secure testing room. Many large test services providers require test centre administrators to be certified in the practice – making sure they are qualified, skilled and knowledgeable about what to look for in the centre, as well as what to do in certain situations.

The Next Level

Physical security aspects aside, perhaps the most secure facet of modern testing and the best defensible method against "Cheating 2.0" is **computerization.** Test items for computer-based testing (CBT) are typically stored electronically and transported to the testing centre in an encrypted state via a secure pipeline directly from the test services provider. When using secure output lines, the possibility of an information breach during transit is extremely low. This process is completely diverse from the transit of standardised paper and pencil exams, which require physical centre shipment through the mail, creating somewhat easier access for cheaters.

With computer-based testing, exams can have multiple forms, thousands more questions to choose from in creating an exam and a random nature that cannot be achieved through paper based testing. Computer-based exams can be leveraged to eliminate the predictability and static nature of paper-based testing, allowing for randomised item presentation, dynamic testing and secure transit of information to and from the testing centre…all facets that make it substantially more difficult for cheaters.

Using a computer to test allows sponsors to consider the incorporation of **performance based items** into their exams. Most exams assess an individual's knowledge through multiple choice questions. Multiple choice items are extremely valuable and will be a critical element of tests for many years, but they may sometimes also be susceptible to 'cheating' (the sharing of potential test questions with another candidate) and 'item harvesting' (the coordinated attempt to collect a large number of test questions and then distribute them for a profit). Supplementing multiple choice items with performance-based ones (tasks that are representative of the activities a candidate might be expected to perform 'on the job') can improve the overall value of the exam while making it virtually impossible to pass the test without a thorough understanding of the material.

Another type of testing that is becoming increasingly used is called Linear on the Fly or LOFT. LOFT is a dynamic forms generation testing model that utilizes "Item Response Theory" statistics to produce an individually assembled exam for each candidate. Success of LOFT exams is highly dependent on having enough items in the item bank to support the model, ideally eight-to-ten times the number required for a psychometrically sound, "normal" computer based test. Concurrently, the method adjusts the item selection routine to account for item exposure, making the memorization of significant portions of the overall exam extremely difficult. The LOFT process ensures that each candidate receives a completely unique and "individualized" exam, making cheating of any type close to impossible.

Certain test service providers also use technology to provide analysis of items and exams to detect abnormalities in the test process. Abnormalities include anything from unusual response patterns or unexpected candidate behaviour (e.g. ending a test early, not completing a test, requesting frequent breaks) to sudden performance improvements -- All of which can be indicators of a potential security concern that can be investigated by a thorough review of the computer files "captured" during a test event.

And then there is Biometrics. As an added security measure some test centres utilize biometric security tactics, such as fingerprint capture. The fingerprint reader, which is the most widely used and accepted practice, captures an image of a fingerprint that is used to monitor the movement of the candidate in and out of the test room. The fingerprint can also be compared electronically to a central database to ensure that the candidate did not test previously under a different name. Should a candidate come back to take another test years later, the information can be pulled up and compared. Additionally, should someone who is NOT said candidate appear at a testing centre years later and claim to be, the centre would be able to tell, from referencing both the fingerprints in the database and the saved identification information, that the candidate is not who he says he is.

Migrating from Cheating 2.0 to Security 3.0

A Boston Globe article last year reported that among 200,000 test attempts there were 1,000 "confirmed" incidences of cheating. The article made quite a big deal about the number, blowing the reality way out of proportion. In fact, this is a rate of a half of one percent. This same story could have just as easily reported the findings differently; that is to say that 99.5 percent of tests are valid and reliable measures of individual skills and abilities.

Despite IT advances that could help candidates cheat on standardized certification exams, testing security has only grown stronger as technology progresses, due largely in part to the rise of large-scale test administrators and the CBT model. Digital video recording systems, biometrics and dynamic exams all work together to stop cheating in its tracks, ensuring that while cheaters may be using "Cheating 2.0," test and test centre security are already on "Security 3.0." In doing so, the very certifications that employees pursue in order to maintain marketability challenge them to prove ethical behaviour as well as knowledge and skill set.

Case Study

You may think, who cares if someone cheats on an exam? Aren't they only hurting themselves? Well, answer this question: Would you want someone who cheated on their nursing exam standing over your child in an operating room? How about someone who didn't really understand accounting fudging your taxes? Or someone who smuggled cheat sheets into a test about construction safety codes building the house your life savings is going into? Would you be willing to risk it? I wouldn't.