Promoting Regulatory Excellence

Thefts, Threats and Cheating: Addressing Security Issues in the Credentialing Process

Presenters: Stacy Lawson, Prometric

Agenda

- Examination of threats to testing integrity—both high and low tech
- For both CBT & PBT Environments, discuss methods & recent trends in:
  - Prevention
  - Detection
  - Response

Threats - Cheating vs. Exam Theft

- Cheating: Can be done by individual or group, usually limited to personal gain only
  - Often low impact to examination program if not widespread or a high stakes professional licensure exam
- Exam Theft: Objective is to remove exam content, or obtain entire exam for wide distribution
  - Can have very high impact if a large amount of the exam is compromised
  - Can result in cancelled future administrations, cost to exam sponsors to republish exams can be several hundred thousand dollars to republish
Common Cheating Methods - Low Tech

- Copying from other examinees
- Cheat sheets hidden in clothes
- Notes or formulas written on hands or legs
- Notes on testing documents
- Notes hidden inside books or testing exhibits
- Notes underneath hats or taped to brim
- Notes inside medicine bottle, water bottle labels
- Notes inside food packages or wrappers
- Accessing notes while on a break/notes hidden in bathroom
- Bribery

Common Cheating Methods - High Tech

- Cell Phones/Text Messages
- I-Phones/Blackberries
- I-Pods- notes & formulas hidden as song names, audio study texts
- Bluetooth ear pieces
- Digital Watches

Common Exam Theft Methods - Low/High Tech

- Sneaking out exam questions on scratch paper or test documents
- Documenting memorized questions while on a break
- Theft of exam question booklets
- Memorization rings, unethical training schools trying to capture actual exams
- Micro cameras - cell phones, pens, buttons, jewelry, etc.
- Audio recorders - mini microphones hidden in clothes
- USB storage devices
- Tampering with test center equipment
Organized Cheating & Exam Theft

- Unethical training schools sending students to steal questions
- Collection of PBT exam booklets
- Sharing of “recalled” questions in study groups, on-line discussion forums, or chat rooms
- Sharing across time zones - Windowed exams
- “Legacy Systems” passed down by college upper classmates
- Proxy Testing- individuals making high quality fake IDs and testing for others

Prevention

Examinee Notification of Test Center Regulations

- Done via exam bulletins, websites, registration confirmation, posters in test center, exhibits during check-in, agreement at beginning of exam, etc.
- No possession of personal items in the test room
- No copying or sharing of exam content by ANY means, to include after the exam
- No disruptive or abusive behavior
- Notification should include penalties for non-compliance - exam invalidation, forfeiture of exam fee, testing ban, revocation of existing status, certification, or license
- Implement a candidate conduct agreement - signed if possible
Test Center Staff- Requirements & Training

- Background Checks- include 5-7 year country criminal search, State Police are an inexpensive option
- Formal Training & Certification Program with annual recertification required
- Exam Administration Policies should be detailed, clear, and reviewed for update twice per year.
- Conflict of Interest Restrictions - NDA
- Performance Incentives for enforcement of security
  - $25 - $50 gift cards for cheaters caught!!
  - Recognition in newsletters or bulletins

Facility- Paper Based Testing

- Separate areas for check-in and testing with restricted access
- All testing materials kept secured by proctor
- Optimum proctor to examinee ratio- 1:20, examinees monitored at all times
- Provide storage for personal belongings, examinees turn pockets out prior to sitting for exam
- Exam booklets numbered, tracked
- Maintain examinee seating chart
- Monitor examinees on breaks

Facility- Computer Based Testing

- Separate area for check-in & enclosed testing room with restricted access
- Viewing window to test room and surveillance system (video & audio recording)
- Signs posted notifying of video & audio recording
- Secure lockers for personal items, examinee keeps key
- Partitions between workstations or privacy screens
- Surveillance cameras view desktops and candidates hands
- ADA compliant
CBT vs. PBT - Security Advantages

- Test items transported to test center in encrypted state via secure pipeline (VPN)
- No risk of lost exam booklets or missing pages
- Locked down PCs, no access to web browsers, USB drives, etc.
- Exams can have multiple forms, randomized item presentation, randomized distracters
- Performance-based testing
- Real-time data forensics to detect suspicious testing patterns and shut down exam or flag for investigation
Examinee Check-In Procedures

- Check-in performed 1:1 by proctor to examinee
- Examinee acknowledges understanding of Test Center Regulations
- Require at least 1 valid, government-issued ID bearing photo & signature, 2nd ID if primary does not have one of these. Use ID Checking Guide if necessary - www.idcheckingguide.com
- Roster/Log sheet to record signature, time in/out, break times, etc.
- All candidate belongings stored
- Issue color-coded scratch paper or erasable note boards
- Candidates made to turn out pockets to prove they’re empty

“Turn Out Pockets Policy”

- In 2008 Prometric tracked over 280 incidents of candidates caught w/ prohibited items in the test room.
- Some were innocent (car keys, hair clips, change, etc.), but many were not (notes, cell phones, etc.)
- After implementing pocket check policy in February 2009 that number dropped to 29 for the rest of the year.

Biometric Identity Management

The candidate’s ID is read on a magnetic stripe and 2D barcode reader which verifies the legitimacy of the government issued ID (North America only).

The candidate’s ID is then placed on a flatbed scanner which captures an electronic image of the photo ID and uses optical character recognition (OCR) to compare printed data and encoded data.

The candidate then places a finger on the fingerprint scanner, which collects a unique physical characteristic which is then linked to the candidate’s identity record.
Detection

• Candidates must be monitored at ALL times
• TCAs available to relieve co-workers if busy with other duties
• Conduct frequent walk-throughs of the test room, focusing on candidates hands and desktops
• Be vigilant for suspicious behavior- going in pockets, watching proctors, excessive breaks, touching equipment
• If possible, monitor candidate activity while on breaks

Proctoring

Surveillance

• Should employ video AND audio with recording, maximum storage possible
• Capable of off-loading recorded evidence to CD/DVD or USB
• Date & Time stamped
• Cameras to cover desktops and examinee hands
• Camera and microphone in check-in area to capture examinee escalations
Surveillance example

Security Audits

- Integrity shopping
- On-site operational reviews & audits
- Remote real time video audits via DVR Surveillance

Emerging Trends in Detection Technology

- Wireless & Internet Jamming Devices
- Cell Phone Detectors - UK Cell Hound
- Hand Held Metal Detectors - Prometric Pilot Underway
Emerging Trends - Data Forensics

- Post-exam score analysis conducted by testing vendors and exam sponsors
- Real-time forensics detecting aberrant testing pattern and flag for investigation or even stop test
  - Aberrant score variances
  - Suspiciously high pass rates
  - High score w/ very short exam duration
  - Multiple examinees selecting exact same answers
  - Web patrolling for posting of recalled questions/brain dumps - www.cyveillance.com

Response

- Have another TCA/proctor confirm the behavior with you
- Escort candidate out of test room to address behavior
- Confiscate all physical evidence notes, prohibited aids, etc.
- Exam sponsor should have policy on whether or not to terminate exam for misconduct
- Call building security or police immediately if examinee becomes disruptive or abusive
- Retain all evidence and surveillance records
- Notify exam sponsor ASAP

Handling Examinee Misconduct
Confiscated Evidence - Chain of Custody

- Document all parties that accessed materials
- If paper, sign & date the back of each sheet
- If a device, record the make, model, & serial #
- Have a security policy to save stolen content on device for prosecution or delete, responsibility on exam sponsor
- Test vendor or exam sponsor may need to obtain signed affidavits from proctor, surveillance footage, and logs
- Always ship materials via traceable method, never use standard mail

Notification to Test Vendor or Exam Sponsor

- Provide same day notification
- Create standard reporting template:
  - Names of all witnesses & contact info
  - Test center ID & location
  - Date & time of incident
  - Examinee name & exam taken
  - Detailed narrative of incident
  - Final disposition- exam finished or terminated?

Test Vendor/Exam Sponsor Response

- Conduct interview with proctor
- Collect all written reports and confiscated evidence (originals to go to exam sponsor)
- Request proctor to testify in disciplinary hearing
- Implement re-training or corrective action if procedural lapses were present
Final Disposition of Examinee could include:

- Exam invalidation, forfeiture of exam fee
- Temporary or permanent testing ban
- Revocation of existing certifications or license
- Notification to employer (Financial or Insurance fields)
- If violation includes theft or disclosure of exam content, criminal or civil charges may be filed

Questions?
Stacy Lawson
Team Leader, Healthcare Segment
Prometric
stacy.lawson@prometric.com