Caveon Webinar Series:

Exam Integrity Investigations: An Introduction to the Essentials

January 21, 2015

CAVEON
INVESTIGATIVE SERVICES

1

About Your Speakers

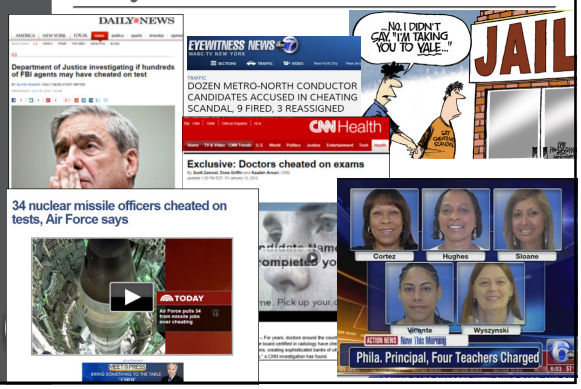
***A. Benjamin Mannes**, CPP, SSI, CHS-III*

***Marc J. Weinstein**, ESQ.*

caveon
Test Security

2

Why We're Here



Yes, this means YOU!

- Certification/Professional Testing (Nonprofit/NGO)
- State Education Departments
- School Districts
- Other government Agencies
- Inspectors General

caveon Test Security

4

Are you Investigating?

- Do you have have an investigative response plan in place to reflexively assess the risk/vulnerability presented by a suspected exam integrity issue?
- Do you have a framework in place to respond to possible issues raised by tipline reports, web searches, and/or data forensic analyses?
- Do you have a comprehensive investigative plan, trained manpower, or the resources to perform these tasks effectively?
- Do you have exam integrity-specific training and/or have had exam integrity added to your SOPs?

caveon Test Security

5

Investigating Cheating: *What you need:*

- Test Security Framework/Program
  - **Threat Assessment**
  - **Staff designee**
  - **Effective policies & agreements**
  - **Effective executive *and* legal support**
- Investigative Framework
  - Detection Methods
    - **Tip lines, Data Forensics, Web Patrol, Vendor notification agreements, Routine Audits, etc.**
  - Investigative response plan
    - **Incident triage**
    - **Who investigates?**
    - **What & when to investigate?**
    - **Evidence Collection (data/physical *and* interviews)**
    - **Evidence preservation**
    - **Reporting**

caveon Test Security

6

If you don't have the framework in place

- Do you have the resources to do this internally (or externally)?
- Have you discussed this with your executive leadership?
  - Do you have corporate buy-in?
  - Are their expectations realistic?
  - Are decisions made based on best practices and exam integrity expertise?
  - Have you started budgeting for this framework?

(*It's always more cost effective to have a plan vs. responding to an incident unprepared*)

caveon Test Security

7

Planning to Investigate: *Test Security Framework/Program*

- **Threat Assessment**
  - Who performs this?
  - What needs to be reviewed?
- **Staff designee**
  - Who investigates possible exam integrity issues, are they assessment staff, a vendor, or an outside agency (Inspector General, etc.)?
- **Effective policies & agreements**
  - What candidate, staff, vendor, and stakeholder agreements are in place?

caveon Test Security

8

Planning to Investigate: *Effective executive and legal support*

- **Effective executive support**
  - Who decides to investigate?
    - Who's recommendation is it based on?
    - How are potential internal disagreements resolved?
  - How are investigations budgeted (staff, resources, & funding?)
  - Are organizational priorities clearly supporting the goals of an investigation?
- **Effective legal support**
  - Is legal consultation with the appropriate counsel?
    - Skill set is not just that of education, but of intellectual property, criminal law, contracts, and white collar investigations.
    - Is it cost effective?

caveon Test Security

9

Investigative Framework: *Detection Methods*

- Use of sources/tip lines
- Online/social intelligence
- Data forensic/psychometric auditing (scoring)
  - Statistical analysis
  - Erasure Analysis
  - Other methods
- "Surveys"
- Performance auditing – spot checking
  - Site visits/secret shopper/exam-day observation
- Interviews of employees/students/candidates
  - Interviewers should be trained investigators

10

Investigative Framework

After Detecting Evidence of Cheating, What is the Investigative Process?

1. Identify investigative goals
2. Identify the evidence available
3. Preserve, gather and document evidence
4. Report findings & make recommendations

caveon Test Security

11

Investigative Framework

Investigative Goals

1. Ensure validity of exam results
2. Identify and punish cheaters
3. Preserve integrity, meaning and value of assessment, certification, license or credential
4. Restore or build public confidence
5. Deter cheating

caveon Test Security

12

Investigative Response Planning

Draft an investigations plan that includes the following essential components:

1. Establish investigative goals
2. Create timeline for investigation
3. Identify all participants in investigation and scope of duties for each
4. Identify and prioritize documentary and physical evidence to preserve and collect
5. Identify witnesses to be interviewed and establish order of interviews
6. Determine the method of reporting conclusions and findings to the organization

caveon Test Security

13

Investigative Response Planning: *Incident Triage*

- After detection, what steps are taken next?
  - How can you decide what type of investigation is warranted?
  - Preliminary Investigation
- Are the allegations substantiated enough to invest investigative resources?
  - If so, are the allegations severe enough to warrant investigation or referral?
- Preserving initial evidence?
  - Anything that may be time-sensitive/subject to disposal
- Reporting the results of your Preliminary Investigation
  - Making recommendations to leadership in a stepwise, detailed approach.

caveon Test Security

14

Investigative Response Planning: *What & When to Investigate*

- What is the scope of investigation?
- Is a performance audit more suitable than an investigation?
- How important is confidentiality?

caveon Test Security

15

Investigative Response Planning: *Evidence Collection & Preservation*

- Preserve all potentially relevant documents and electronically stored information ("ESI")
- Issue evidence hold memo to all potential witnesses and custodians for documents and ESI
- Advise all potential witnesses to maintain confidentiality of investigation and NOT to discuss the subject of the investigation with each other

caveon Test Security

16

Investigative Response Planning: *Evidence Collection & Preservation*

Ensure admissibility of evidence in potential future proceedings by preserving the chain of custody, as follows:

1. Identify source of evidence
2. Record date, time and location of where evidence was collected
3. Identify person that collected evidence, as well as any witnesses of the process
4. Establish where evidence is taken and by whom, as well as how evidence is secured for the duration of the investigation
5. Keep evidence in a secure location, with limited access, and make a record every time a person accesses the evidence
6. Create a written record of all steps in the process

caveon Test Security

17

Conducting Investigations

Identify, Gather and Preserve Available Evidence

- Data forensics and analytics, including score history
- Documentation of testing procedures and participants, including seating charts and chain of custody documents for test and answer documents
- Video and/or audio surveillance of test center
- Biometric data for examinees
- Test center admittance and break logs
- Tipster statements
- Electronic evidence, including but not limited to cell phone images, text messages, call records & emails
- Social media and other information posted online
- Interviews of witnesses

caveon Test Security

18

Investigative Response Planning: *Reporting*

Written Report or In-Person Presentation of Findings?

- Likelihood of public disclosure and/or scrutiny by media?
- Likelihood that report could be produced to a third party in discovery?
- Intend to provide report to a government agency?
- Need to tell the organization's story about the matter?
- Does the test sponsor need a roadmap for further action in response to findings?

caveon Test Security

19

Investigative Response Planning: *Reporting*

What Level of Detail Should be Included in the Written Report?

- Report could be written at a high level to summarize findings or in granular detail
- Consider including the following components:

1. Introduction
2. Description of events that triggered the investigation
3. Description of the investigative methodology
4. Concise statement of specific findings of the investigation
5. Summary of all evidence gathered
6. Identify each person who engaged in wrongdoing and describe what, if any, laws, regulations, and/or policies each person violated
7. Identify possible courses of action for organization

20

Investigative Response Planning: *Reporting*

- **Be factual**, not conclusory
- **Detailed evidence included in an addendum** with chain of custody
- **Incident response recommendations** can be made consistent with your policies

caveon Test Security

21

Investigative Response Planning: *Reporting*

- Use a confidential memorandum for improvement recommendations
  - **separate from the report of investigative findings**.
- Questions to be addressed:
  - Was a **security vulnerability identified** during the incident?
  - If so, **what can be done to change** policies, procedures, or technologies to **better deter or detect** it?
  - Are there **other ramifications** to the organization from the incident?

caveon Test Security

22

Updating the Plan: *Separate after-action reporting*

- Lessons learned
- Process improvement
- Mitigation and Prevention
  - What internal process changes could have prevented this type of exam integrity issue in the future?
- Executive discussion

caveon Test Security

23

Join us at ATP and Online

- **Security at the Forefront** – March 2nd, 4 PM
- **Exam Security Incident Response Workshop** – March 3rd, 8:30 AM
- **Working a Case: Best Practices in Conducting Exam Integrity Investigations** – March 4th, 11:30 AM
- *Twitter:* **@ExamIntegrity**
- LinkedIn Groups: **Exam Integrity, ATP Test Security**

caveon Test Security

24

Thank you

Ben Mannes
ben.mannes@caveon.com

Marc Weinstein
marc.weinstein@caveon.com

- LinkedIn Group – Test Security
- Follow Caveon on twitter @caveon
- Check out our blog…www.caveon.com/blog/
- LinkedIn Group – Caveon Test Security

caveon™ Test Security

25