Session #2 He said she said

A customer reports that a folder belonging to another company was mailed to them inadvertently by your company. As the security officer, you are asked to investigate this breach.

Who do you need to involve from the ITP? Explain your answers?

- Legal
- Compliance
- Security
- Human Resources
- C-Suite representatives to include representative of the Chief Trust Officer or Chief Information Security Officer
- IT Operations
- Security Engineering
- Finance
- Product Management
- Science and Technology
- Business Operations
- Media

You interview the staff, and everyone denies it. What other resources may be at your disposal to investigate the incident and find the culprit? (Logs, cameras, badge readers, etc.)

What insider threat behaviors has the negligent employee displayed?

a. Access attributes (privileged users, access to proprietary information, leadership, etc.).

b. Professional lifecycle and performance (complaints, substandard work, disgruntled employee, unauthorized absence, etc.).

c. Foreign Considerations (Foreign government interests, foreign assets, receiving benefits from foreign nation).

d. Security and compliance history (security/compliance violations, non-compliance, negligence, misuse of privileges, etc.).

e. Technical activity (violating acceptable user policy, anomalies in data usage or exfiltration, unusual data access request, etc.).

f. Criminal, violent, or abusive behavior (threats to employees or company, criminal activity, sexual assault, or harassment).

g. Substance abuse issues (drinking on the job, Illegal substance use, drug test failure).

h. Financial considerations (debt suddenly is cleared up, unexplained affluence after long periods of debt, financial crimes, etc.).

i. Judgement and Character Issues (falsifying employment information or data, anti-social and compulsive behavior, endorsing workplace violence or abuse, past lack of candor.