Investigative Process for Incident Investigations

Investigative protocols should be approved by executive management in order to lend credibility and authority to the process, regardless of whether the organization has a separate IU or full-time investigator. A protocol should generally include a decision logic matrix to quickly identify who has responsibility for the inquiry, who should be notified, and whether immediate referral to law enforcement or the legal department is appropriate. The protocol should then outline the prescribed investigative steps.

The following sample provides a general idea of recommended contents for a protocol:

- Assess the credibility of the source of the information and the information itself.
- Determine whether physical evidence is present and warrants collection (i.e., is there a scene to be processed?).
- Conduct initial witness interviews.
  - Give priority to those who were directly involved in the incident or may have perishable information.
  - Give priority to those individuals who may not be available later for interview (e.g., visitors, employees scheduled for a trip or reassignment, informants only temporarily in the area, etc.).
  - Get recommendations for follow-on interviewees (i.e., find out who else should be interviewed and obtain identifying or contact information for them).
- Document individuals (witnesses, bystanders, etc.) who declined to be interviewed or who were not available for interview.
- Document other potentially relevant situational or environmental conditions.
- List all security, corporate staff, and other officials who were involved in the initial response, assessment, and investigative steps.
- Conduct third-party interviews (of individuals or agencies that did not witness the incident or were not present but may have relevant information).
- Check security and investigations indices or databases for relevant information.
- Make and document all notifications regarding the incident.
- Determine information gaps, and identify sources or methods to fill the gaps (via interviews, evidence collection, surveillance, observation, investigative research, records checks, etc.).
- Recommend follow-on action or referral.
- Complete appropriate documentation and database entry.

Security officers and staff should receive training on applicable investigative protocols, including the need to protect investigative information. Particular care should be taken with hot line or complaint calls. Callers should be made to feel that the information they provided is important and appreciated and that the matter will be looked into. Failure to do so may discourage future reporting of valuable information. At the same time, potentially sensitive information must not be provided to complainants or others because complaints may lead to the initiation of undercover operations or other investigative activities that must be kept confidential.

The report of investigation for this type of inquiry is often a standardized form. It is particularly important that reports be properly filed or entered in a database so the information they contain is retrievable later. The report should note whether a follow-up is required or recommended and whether referral to the IU or an outside investigative services firm or law enforcement agency is advisable or required.

1.4.2 MISCONDUCT INVESTIGATIONS

An important subcategory of constructive incident investigations is the misconduct investigation. This is generally an internal investigation conducted when an employee or other individual closely affiliated with the organization is suspected of violating a written corporate policy, a directive, terms of employment, or a federal, state, or local law.

An important characteristic of workplace misconduct investigations is that they leave the employer particularly open to legal action by employees or former employees who feel they have been treated unfairly. Among the alleged causes for legal action are discrimination, wrongful termination, sexual harassment, defamation, and false arrest. The best way to prepare for such investigations is to coordinate the matter as soon as possible with the human resources director and corporate legal counsel (or equivalent officials). This recommendation pertains to most types of private sector investigations but is particularly important in employee misconduct cases.

Investigative Techniques and Issues in Misconduct Cases

In general, those involved in a misconduct investigation should consider the differing perspectives of the parties on both sides—complainant and subject. From the employer's perspective, the issue is a routine policy or disciplinary matter. From the subject's perspective, it may be traumatic situation. Subjects may feel their career, livelihood, and reputation are at risk.

Experienced corporate investigators do not use techniques that may induce an innocent person to confess to guilt. The use of coercive interview techniques can significantly impair

the reputation of fairness in a corporate setting—and thus damage the credibility of and confidence in the IU and individual investigator. Some individuals are easily intimidated and, although innocent, may confess to crimes and wrongdoing when confronted with unfounded promises of leniency or fabricated and supposedly overwhelming evidence. The use of inappropriate techniques and failure to protect personal or confidential information during the investigation can lead to embarrassment for the corporation, erroneous investigative conclusions, and lawsuits against the enterprise.

Suggested practices in misconduct investigations include the following:

- Determine the proposed outcome or disciplinary action (should the allegation be proven) at the outset of the investigation. This helps prevent claims of personal discrimination or the appearance that the intended action was modified during the course of the investigation based on what or who was shown to be involved.
- Use information sources both internal and external to the organization to help prove or disprove allegations. Relying solely on internal sources may limit the scope of the information collected and may conceal critical facts or data points.
- Gather relevant information from previous employers of the individual in question. The information may show patterns of behavior and reveal significant data that can be used to direct the investigative efforts, strengthen the case, explain existing known facts, and provide additional leads. High turnover rates, common today, make it even more important to conduct thorough background checks and consider interviewing past coworkers, supervisors, colleagues, and other associates.
- Even in cases not involving IT system abuse, consider collecting electronic evidence, such as e-mail records, access requests, logons, file downloads, and remote access sessions. These sometimes overlooked sources can provide valuable information.

Finally, the potential side effects of a misconduct investigation and the way in which it is conducted must be considered. For example, when deciding to use surveillance (covert monitoring to gather intelligence) it is important to remember that it is difficult and vulnerable to discovery if conducted while moving. However, an overt surveillance, whose main goal is to prevent crime or misconduct, may be effective. Effects may include diminished workforce productivity, strained interoffice relationships, and threats and intimidation. An internal investigation (or even a rumor of one) may turn coworker against coworker, create other frictions in the office, and have a short- or long-term impact on workplace comfort level and trust relationships. Although the potential for side effects cannot be allowed to dictate the aggressiveness or outcome of an internal investigation, it should be considered in terms of the overall investigative strategy, information dissemination, treatment of individuals, and professional demeanor of those involved in the case.