

# Avoiding Pitfalls in Internal Investigations

Internal investigations play a critical role in mitigating insider risks, and technology is making the job of investigators easier. Nevertheless, organizations can make missteps that jeopardize the effectiveness of investigations.

StoneTurn Partner Mike Roos explains how to avoid those pitfalls.



## What are the critical elements of an internal investigation?

While every investigation is different, getting it right requires structuring the effort around five critical elements:

- 1 First, an organization needs to have a clear understanding of the main objectives of the investigation, whether that is disciplinary measures, legal action or eventually to make a report to regulators. Once the objectives are understood, the next step is assembling a team with the requisite expertise and experience to undertake the investigation. Consideration should be given to whether legal privilege is necessary to protect the results of the investigation, the geographic expanse of the investigation and any special expertise required, such as computer forensics or linguistic profiling.
- 2

- 3 Next is securing all forms of evidence and protecting the chain of custody. Security of evidence in an investigation is important whether the investigation becomes a criminal matter or not. Organizations should gather all forms of evidence, whether digital or paper, in a way that lets them secure the evidence and trace back how and from whom they obtained it.

### Investigations: A Checklist


- Understand the objective
- Assemble an expert team
- Secure the evidence
- Document review, data analysis
- Interviews



- 4 Undertaking a document review and doing analysis both require well-documented and methodical processes to avoid missing information critical to the investigation.

The documentation should include protocols to ensure consistency across all reviewers, in the event a document review tool is utilized, and an understanding of the nature of the information sought from each device or repository.

- 5 Lastly, most, if not all internal investigations will involve interviews. Before undertaking interviews, it is important to determine how the investigators will represent themselves to the interviewees, whether any special admonitions must be given prior to commencing the interview, the substance desired from each interviewee and the documents that the interviewee would be shown during the interview.



## What are some of the frequent mistakes made conducting internal investigations?

One of the more common ones we see is institutional bias. People within every organization have biases, and a common one that can derail investigations is the notion, “Surely this couldn’t happen at my organization.” Disbelief that fraud is a possibility is a problem for internally conducted investigations, which is why engaging a third party makes sense—bringing more objectivity to the process.



Another pitfall is lack of buy-in from senior management. Investigators need access to information, and a stakeholder who is lower in the chain of command can present a roadblock without a senior leader being available to clear the way. For that reason, an investigation should be sponsored by a senior executive, such as the general counsel or a member of the audit committee, who can help ensure that needs of the investigation, such as IT access or document requests, or access to employees are met timely and completely.

Obviously, this stakeholder must be trustworthy and gauging that trust can sometimes be tricky. Let me give you an example: In one accounting fraud case, a multinational holding company had inflated its profits by billions of dollars over an eight-year period. The ensuing investigation determined the rogue party was the company’s chief executive officer, who had handpicked board members he knew wouldn’t challenge him. A reminder that just because the internal stakeholder is senior, doesn’t mean you should let your guard down. At all times, investigators must have a 360-degree view of the organization—risk can be lurking anywhere.

Misaligned agendas are another pitfall. It’s important that everyone involved in an investigation be aligned regarding the objectives of the investigation. One of the roadblocks we typically see here is management trying to save money and limit the scope of an investigation.

Tying back to biases, on a similar note, assumptions can be problematic in investigations. Organizations may zero in on one issue or person without considering the larger picture or implications, including what the actual issue is. A deleted email, for example, might lead the organization to suspect the account holder, when that might not necessarily be the case. Bringing in



an experienced third party, with investigators who are familiar with a number of different fraud scenarios and have learned through experience to apply skepticism, for example, can prevent incorrect assumptions from fouling up an investigation.



## How have insider investigations changed in the past few years?

Technology has changed investigations a lot. Twenty years ago, everything was paper based. In just the past few years, nearly all the evidence in investigations I have led has been in digital format. Most of our investigations over the last two or three years have not involved a physical “paper trail.”

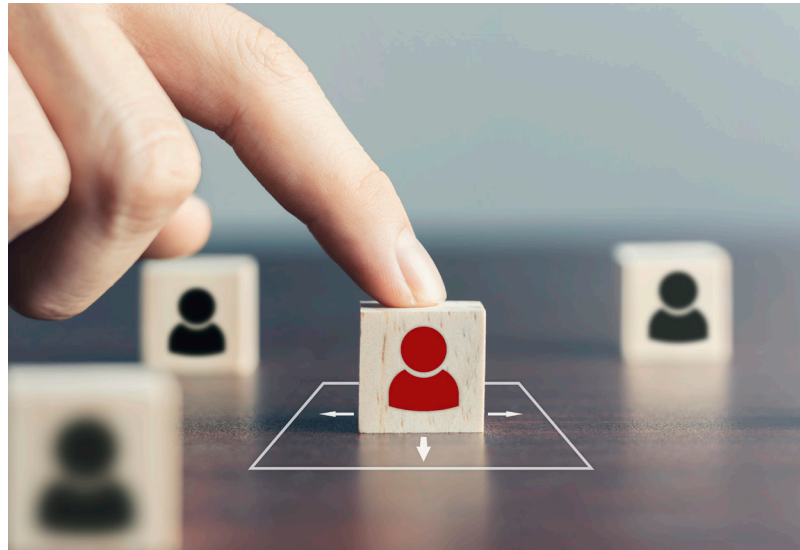
**Twenty years ago, everything was paper based. In just the past few years, nearly all the evidence in investigations I have led has been in digital format.**

Evidence is now more likely found on laptops, in email, on smartphones, and in apps. Personal messages and location tracking can be highly useful resources for investigators. Look around and it's easy to see almost everyone has a phone in their hand: what you may not realize is that activity creates

trails of evidence. In our investigations today, having access to a suspect's laptop is good, but having access to a mobile device is typically where the really meaningful evidence can be found.

That said, while technology has helped resolve investigations, technology advances also have enhanced the ability to commit fraud. Remote work, combined with malintent and personal devices, have given bad actors a sense of distance from those who might be watching. Without the right precautions in place, for example, VPNs, blocked USB ports and the disabling of screen captures, those desiring to

commit fraud will feel more comfortable to do so remotely, as opposed to while sitting in an office next to co-workers.



**At the end of the day, a rogue insider is like a chameleon—they'll blend in to match any environment. Circumstances will change, and so will the avenues bad actors take to exploit them. Yet, having a strong foundation to any investigation, with the right team of experts, will allow organizations to more holistically identify the root of the problem and remediate it.**

