exterro®

DIGITAL FORENSICS CHECKLIST

Don't Let Departing Employees Turn into Insider Threats

How to Conduct an Effective Internal Investigation

While ransomware attacks and data breaches are justifiably scary, insider threats are far more common—and far more damaging—than most people know. Culprits like the "London Whale," who cost JP Morgan over **$7 billion,** and the Yahoo research scientist who stole over half a million pages of IP after taking a job from a competitor make headlines too, but such malfeasance often goes undetected until it's far too late.

Installing a digital forensic investigation process like the one laid out in this checklist can help you quickly and efficiently assess whether a departing employee is a threat to your organization.

Determine Scope of Investigation | Set the Window of Time for Review | Preserve Relevant Data | Evaluate the Evidence and Prepare Report

Step One:
Determine the Scope of the Investigation

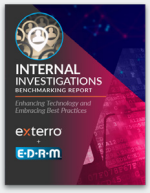
Before you begin examining the employee's devices and network activity, learn about their standard duties and role from their supervisor and/or human resources. This will help you identify any actions, data, or artifacts that look out of the ordinary.

- ◯ What software do they use?
- ◯ What accounts and permissions do they hold?
- ◯ What data do they routinely access?
- ◯ Does the employee work from home, an office, or hybrid?
- ◯ Does the employee travel for work?

Step Two:
Set the Window of Time for Review

Determine how long prior to the employee's departure you want to consider in your investigation. Computers and web applications can store years' worth of history—but it's not feasible to review that much data.

- ◯ Consider events, like evaluations, performance reviews, warnings, other HR actions, and promotion decisions that might cause a major shift in the employee's mental state.
- ◯ Often a 60- to 90-day window gives you time to see the employee's normal routine.
- ◯ Pay attention to the "wind down" period and note any deviations from the employee's routine.
- ◯ Note any **extreme changes** in behavior or suspicious activity like:
  - » File or data deletions
  - » File or data copying
  - » Mounted USB drives or other devices



Learn how other organizations are leveraging internal investigation technology and processes in Exterro and EDRM's: Internal Investigations Benchmarking Report

Step Three:
Preserve Relevant Data

Storage is cheap and questions are expensive. What you don't know can end up costing you, so make sure to preserve the information you need. Use these questions to determine what you preserve and for how long.

- ◯ Set and follow a policy for processing employees' primary workstations. Imaging the drive offers more flexibility and is often the best solution, but other options are:
  - » Retain the machine intact for analysis
  - » Remove and replace the hard drives
- ◯ Do not reformat or reissue devices if there's any possibility of employee malfeasance and therefore the need to investigate.
- ◯ Set and implement policies for other employee devices and accounts, such as:
  - » Company-issued and BYOD smartphones
  - » Cloud software platforms
  - » Cloud storage platforms
  - » Chat or instant messaging applications
- ◯ Don't delete ex-employees' cloud accounts or storage too fast. Once the data is lost, it's gone for good.

Step Four:
Evaluate the Evidence and Prepare Your Report

Once you've gathered the relevant data, it's time to conduct the actual investigation. Look for changes in user behavior, applications used, event logs, and other artifacts that differ from the employee's routine and responsibilities.

- ◯ Are there any unusual files on the machine? Any files that should be present but are not?
- ◯ Does the file and application history show anything abnormal or concerning?
- ◯ Does anything in the web history cause concerns—changes in cloud access, uploads, downloads, or web-based communications?
- ◯ Review the event log for any unauthorized or unusual devices mounted, logins or logoffs, or remote access to the machine?
- ◯ Lean into your expertise and interpret the evidence and deliver your conclusions in a well-documented report.