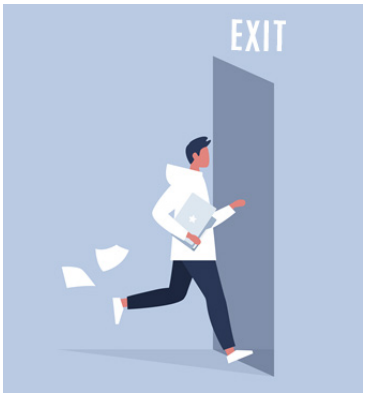
Departing Employee Forensic Investigations

Using Computer Forensics to Investigate Employee Data Theft



When employees leave your employ, they may take valuable electronic files belonging to your organization. If they go to work for a competitor, this can often lead to the competitor gaining an unfair advantage.

All departing employees pose a risk of data loss or theft, most commonly occurring with executives, management, sales, marketing, R&D and engineering positions. In fact, by some estimates, 70% of the value of publicly traded companies is intellectual property in the form of patents, copyrights, trade secrets, financials, formulas, customer & vendor lists, plans/strategies and more. Any disgruntled employee, or one seeking a 'leg up' at their new company, is a suspect.

Telltale Signs An Employer Should Look For

Signs that an employee departure may warrant an investigation include unsual employee activity, such as:

- Plugging a personal USB thumb drive or hard drive into a computer
- Arriving to work at odd hours or establishing remote desktop connections during off-hours
- Transferring large amounts of data on the company network
- Visiting file sharing sites like Dropbox or Google Drive
- Sending emails with attachments to personal accounts

What can an employer do if there are concerns of this activity?

Do not repurpose or tamper with the devices in any way. Don't even turn them on or off. It could delete important digital content or artifacts that provide relevant evidence!

Instead, include Digital Forensic Preservation in your Employee Departure Program. By incorporating Vestige's digital forensic experts as part of your employee off-boarding routine, you can get to the truth quickly before extensive damage can take place. Vestige's forensics experts will preserve digital evidence from all devices and perform effective discovery to uncover any relevant digital evidence that is admissible in court, should litigation become necessary.

Vestige OaaS

The Vestige forensic team provides Offboarding as a Service (OaaS) as a turn-key eDiscovery preservation protocol for preserving legal-hold data from departing employees for corporations who want to be proactive in collecting, preserving and analyzing vital data from these employees.

Vestige **Employee Departure Program**

Employees depart organizations all the time, it is a normal occurrence. However, the question arises as to what should be done with those employees' devices and more importantly, their data. Vestige's Employee Departure Program works to understand your organization's policies regarding the disposition of employees' equipment and data upon their departure. Vestige then works with you to put a plan in place to secure data for current litigation matters or future investigations.

Step 1 – Consultation Regarding Departing Employee Process

Vestige consults with client legal, HR and IT teams to understand the process by which information is communicated upon an employee's departure. Vestige works to ensure that proper lines of communication are in place to prevent the accidental wiping of employee devices prior to consideration of litigation holds or investigations. Vestige looks to understand the process by which devices, mailboxes and shared data is redistributed or reassigned upon an employee's departure. Vestige then puts together a plan, agreed upon by all stake holders, as to how the process should take place.

Step 2 – Reduction of Data

Vestige works with client IT to produce hash sets of base laptop, server and desktop configurations and keeps those hash sets updated over time. The creation of these hash sets allows for quick elimination of non-relevant data from preserved client forensic images to streamline processing and analysis.

Step 3 – Remote Preservation of Devices

Following the completion of Step 1, Vestige puts in place mechanisms by which Vestige assists in the remote preservation of workstations, server shares, cloud storage, mailboxes and mobile devices upon an employee's departure. As employees depart, the client will have a checklist for contacting Vestige to initiate the remote preservation. Cost is dependent on device and is per device.

Best Practices to Perform for Every Departing Employee

It is best practice to incorporate preservation of all digital device data as it ensures business continuity and adherence to Information Governance policies. Our suggestions:

- Organize, secure and archive potential evidence images
- Utilize Vestige's OaaS forensic collection and preservation service for every departing employee's digital devices.
- Host relevant metadata in a secure cloud-based environment. This enables secure early case assessment and promotion of relevant data for review and analysis of data including smartphone data, computer activity and geolocation for any potential internal investigation that requires digital evidence.
- Finally, from preservation to presentation, by implementing best practices it is easy, cost efficient and displays the whole story should an internal investigation be required.

Contact Vestige today to discuss your Employee Departure Program

TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™

info@VestigeLtd.com | **800.314.4357** | www.VestigeLtd.com

02112021