Getting Started: **4 Steps** to Simplifying Employee Investigations

Veriato

www.veriato.com

The biggest challenge to investigations is getting the right data.

If every employee simply focused on their work, investigations wouldn't be necessary. But, that's simply not reality. Employees spend time addressing personal issues while at work. They interact with others in ways not sanctioned by the organization. And, in dire circumstances, refocus their alignment with the organization onto themselves, looking for ways to take advantage of company data, assets, resources, and money.

The whole point of an employee investigation is for the organization to understand whether the employee did something wrong or not. And, if evidence points to improper behavior, knowing exactly what transpired will be necessary to determine scope, impact, and response.

The greatest challenge for most organizations is visibility into employee behavior and actions. Without it, your employee investigations will be anything but simple.

Veriato provides contextual user activity detail and screen recordings needed to investigate whether employee activity is appropriate, sanctioned, and well-intended. By logging all user activity and capturing screen detail for video playback, Veriato creates an indisputable audit trail that can provide context around what transpired, who did it, and, in many cases, why – all making your investigative efforts materially easier.

Introduction

While most organizations with a mature HR department are aware of the need for investigations, being able to perform one is something that falls squarely upon IT. Requests for data from disparate systems, timeframes going back years, and seemingly "easy" required details that are nearly impossible for IT to deliver.

So, what's needed is a formal investigation plan in place with defined goals, methods, processes, and people that works to proactively ensure the necessary behavior and activity data is available should an investigation be necessary.

This Getting Started brief provides some high-level guidance around the steps necessary to implement an employee investigation process. While not exhaustive, it does lay the groundwork for you to begin planning and rolling out an investigation program, complete with desired solutions.

STEP 1

Identify Necessary Investigations

There are a number of employee-related issues that can occur requiring the attention of HR, IT, and Legal. But each organization has its own level of concern about each, which impacts whether investigations are necessary or not. Additionally, as you'll see later in this paper, the data necessary to successfully carry out an investigation – depending on the scenario in question – may differ. So, it's important to begin with identifying which scenarios will require investigations within your organization.

In general, there are 4 scenarios in which you may want to perform an employee investigation:

1. **Insider Data Theft** – Data breaches are perpetrated by insiders 28% of the time[1]. With an average breach size of a little over 24,000 records[2] and an average cost/record of $141[2], the average cost of a data breach is slightly under $3.4 Million[2]

2. **Corporate Fraud** – According to the Association of Certified Fraud Examiners[3], the median loss from fraud is $130,000, taking 16 months to be discovered. With 85% of perpetrators being first-time fraudsters.

3. **Harassment / Discrimination Complaints** – An employee acting inappropriately in the workplace can have serious financial repercussions. The EEOC reports that over 84,000 harassment and discrimination charges occurred in 2017 with damages in excess of $355 Million.

4. **Unproductive Employees** – Employees are the lifeblood of your organization. And the loss of focus on productive work can quickly translate into a material cost to the business. The simple act of each employee wasting an hour a week surfing the web can cost you. In a 100-person company, if each employee wasted an hour weekly, this equates annually to 2 and a half employee's time normally put into work-related activities. In essence, you're conceptually paying for 2.5 employees to do literally nothing work-related all year.

---

[1] *Verizon, Data Breach Investigations Report (2018)*
[2] *Ponemon, Cost of a Data Breach Report (2017)*
[3] *ACFE, Report to the Nations (2018)*

STEP 2

Determine Needed Activity Data

For each investigation scenario, you need to determine the specific kinds of employee activities that will yield sufficient evidence to determine whether any kind of inappropriate employee action(s) exist. These should be tactical activities performed by employees that, in sum total, provide information and context for a given investigation.

In general, the following kinds of activity data is helpful as part of an investigation:

- **Application Usage** (Computer) – The applications used by an employee and actions taken within those applications provide key insight into activity that may hurt the organization. Focus on which applications are used, how long, and, if possible, go down to the level of what actions were taken within the application. Note that most applications don't provide an audit trail, so you may need to look at third-party solutions to accomplish this.

- **Data Interaction** (Computer) – In cases of fraud or data theft, even just opening a data file can provide valuable insight into which employees may be probable suspects. Having an ability to know who accesses, viewed, copied, or printed data – regardless of application – is key. Additionally, visibility into the use of USB devices, cloud storage, and any other application that performs file transfers (e.g. Skype) is necessary.

- **Web Usage** (Computer) – Where an employee goes on the Internet indicates what's important to them. If they spend a lot of time on job sites, you know they're looking for a job. If on Social Media (and assuming that's not part of their role), you know they're wasting time. You need visibility into websites visited, searches made, as well as any use of cloud storage and web-based email.

- **Web Usage** (Computer) – Employees are the lifeblood of your organization. And the loss of focus on productive work can quickly translate into a material cost to the business. The simple act of each employee wasting an hour a week surfing the web can cost you. In a 100-person company, if each employee wasted an hour weekly, this equates annually to 2 and a half employee's time normally put into work-related activities. In essence, you're conceptually paying for 2.5 employees to do literally nothing work-related all year.

- **Communications** (Computer, Phone) – Having specific detail on what an employee communicates establishes what was said, to whom, and provides great context around other activities. For example, take a user printing out company financials. The presence of an email from the CFO asking them to do so provides context around the action, further aiding an investigation. You should have an archive of any corporate email and chat applications, call detail and, potentially, recording of phone conversations, and, if possible, detail around the use of any web-based email and social media-based communications.

- **Badge Scans** (Physical) – In cases where the security of company assets is in question, having an understanding of when an employee is within the building, where they went, etc. can help establish physical proximity as part of an overall investigation.

The table below demonstrates which of these is useful in each investigation.

	Productivity	H/D Complaints	Fraud	Data Theft
Application Usage	✓		✓	✓
Communications		✓	✓	✓
Data Interaction			✓	✓
Web Usage	✓		✓	✓
Badge Scans		✓	✓	✓

STEP 3

Identify Solutions to Assist

Because any native tools provided by operating system or application vendors is likely not designed specifically for investigations, it's far more probable that you will need to purchase one or more third-party solutions to address your investigation needs.

There are a number of solution types to consider, each with their pros and cons.

- **eDiscovery Solutions** (Proactive) – The process of identifying, collecting, processing, preserving and retrieving data and email that may be a part of legal matters falls under the umbrella of eDiscovery. These types of solutions focus on ensuring relevant data and communications can be found when needed to address an issue.

  PROS These solutions are designed to keep data from being modified (ensuring the integrity of the data collected), and, as the name implies, make the discovery of pertinent information easy to find.

  CONS The data collected is limited in scope and provide no details around employee activity. eDiscovery solutions are best suited for legal- or HR-related matters.

- **Event Auditing Solutions** (Reactive) – Because many applications, operating systems, and security systems all generate log data, it's conceivable that you can consolidate this information into a Security Information Event Management (SIEM) solution. Many SIEM solutions already support a multitude of data sources, with an ability to leverage standard data formats to accommodate any data source outliers.

  PROS SIEM solutions can pull from a wide range of data sources, giving you a breadth of visibility across many types of systems and platforms

  CONS Many SIEM solutions require a material amount of configuration to provide you with valuable insight. Additionally, a SIEM's value is reliant upon the level of audit detail available. So if your investigation requires information from an application what has no audit trail, a SIEM will provide little value.

- **Forensics-Focused Solutions** (Reactive) – These solutions are designed to dig into the details after an event has occurred. With an ability to work with multiple machines, both on and off the network, these solutions automate all the dirty work of collecting and making sense of forensics data left on a wide range of devices.

  PROS These types of solutions are a great answer in circumstances where you have no proactive measures in place. They have deep expertise into the operating systems, applications, and email platforms they interact with, in order to pull out as much valuable detail possible.

  CONS The value of the investigation is highly reliant on the forensic artifacts left behind. There is no visibility into specific actions that occurred, with the exception of that which can be determined from the artifacts. For example, Forensics can tell you the employee went to a particular website (if browser history is intact) but won't necessarily be able to tell you what they did while visiting the site.

- **User Behavior Analytics** (Proactive) – These solutions look for shifts in behavior and/or activity as leading indicators of risk, alerting the appropriate people to a potential threat. For example, is an employee begins to become negative about the company and their job, the organization can be notified, with steps taken to monitor the user's activity for productivity loss or threatening behavior.

  PROS Unlike the other solution types, this one is specifically designed around looking for leading indicators before an action threatening to the company takes place. In some cases, detailed activity data can also be collected for review to see if threatening behavior has already taken place.

  CONS Not all UBA solutions are based on the same data types. Some are user endpoint-based, while others are more SIEM-like, relying on the addition of analytics to identify suspect behavior.

The table below demonstrates which of these solutions is useful in each investigation.

	Productivity	H/D Complaints	Fraud	Data Theft
eDiscovery		✓		
Event Auditing	✓		✓	✓
Forensics			✓	✓
User Behavior Analysis			✓	✓
User Activity Monitoring	✓	✓	✓	✓

STEP 4

Develop Your Incident Response Investigation Plan

The moment the organization is aware of a potential employee situation (whether via HR, Legal, or IT), there needs to be an investigation plan in place. The plan, regardless of the kind of solution(s) you have in place, should be broken down into a few aspects:

- **Scenarios** – Define specific investigation scenarios and develop plans accordingly. At a minimum, use the four previously listed in this paper. You may also want to dive a bit deeper into each of the 4 and develop specific plans around certain kinds of actions, threats, or scenario details.

- **Alerts** – Define who will receive any alerts generated by your chosen solution(s). Logical initial choices include IT and HR but should be defined based on the specific capabilities of your implemented solution(s) and those that will take action based on the alert.

- **Escalation** – Have a process in place for alert recipients to notify the proper team members. Depending on the incident scenario, the processes will likely be different. For example, if the alert comes from a UBA solution denoting someone printing much more than normal, you may want HR to first inquire with the department head if there are any special projects in place requiring excessive printing. But if the alert is from a UAM solution indicating a user copying sales data to a cloud storage service, you may want to notify IT and Security teams so the potential threat action can be stopped immediately.

- **Activity Review** – When a suspect event occurs, you need an approval workflow (likely involving HR) to allow IT to review user activity (should a UAM solution be implemented). The workflow should include how to report the findings and to whom.

- **Response** – The investigation should provide enough context to understand exactly what actions have taken place. A plan involving HR, Security, and IT should be in place to address and coordinate responses like bringing the employee to HR (in the case of a productivity issue), immediate logoff (in the case of a malicious insider committing fraud or stealing data), termination, etc.

Getting your Employee Investigations Started

The steps outlined in this paper provide high-level direction to what will prove to be a bit of leg work to get processes, policies, plans, and solutions in place. Employee investigations are only seen as being difficult because none of the work has been done to proactively track activity in a way that will be useful at the time an investigation is warranted.

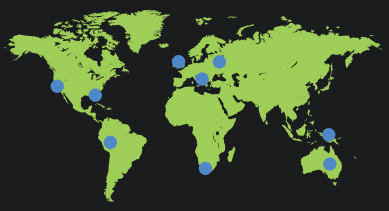
By following the 4 steps to simplify your employee investigations, you can be confident that you will able to not just successfully perform an investigation, but have the detail you require to get the answers you need to act swiftly in the best interest of the organization

Veriato Resources

Veriato 360 Information – Veriato.com/360
Veriato Recon Information – Veriato.com/Recon

To learn more about how Veriato can help you with employee investigation, contact a Veriato representative today.

Over 3,000 enterprises, & thousands of SMBs have placed their trust in our solutions



Our solutions are deployed in **110+ countries**

Veriato USA

4440 PGA Boulevard , Suite 500

Palm Beach Gardens, FL 33410

Veriato EMEA

3rd Floor, Crossweys House

28-30 High Street

Guildford, Surrey

GU1 3EL United Kingdom

https://plus.google.com/+Spectorsoft

https://www.linkedin.com/company/veriato

https://twitter.com/veriato

https://www.youtube.com/SpectorSoft

https://www.facebook.com/VeriatoInc/