Take Charge of Cyber Sleuthing to Make Sure Your Investigation is Done Right

Compliance and Ethics

Let’s suppose you receive a credible report that several employees are colluding to defraud your company. Let’s further suppose that you have no evidence corroborating these allegations. When creating your investigation plan, what should your next steps be? If you confront those accused of misconduct, they are likely to deny any wrongdoing and you’ll be no further along in your investigation. Worse yet, they will know they are being scrutinized and will attempt to destroy evidence of their misdeeds. This is the kind of circumstance in which cyber sleuthing to collect electronic records located in multiple locations may be your only way of determining whether the allegations are true. The following are three steps you might consider taking to maximize your chances of success:

Step 1: Preserve evidence

If your company is like most, email accounts are purged on a periodic basis. So, one of the first things you should do when launching your investigation is to put a hold on the destruction of emails from individuals under suspicion as well as those with whom they may have communicated to perpetrate the fraud.

If you are also concerned that they may destroy evidence on their work computers, but you are not yet prepared to take possession of their equipment, check with your IT department to see if they have the tools necessary to surreptitiously replicate the hard drives of devices when they are connected to your company’s systems. If you go this route, be sure you understand the associated risks and limitations. With some systems, there is a possibility that a cyber-savvy suspect may detect their computer is being hacked. If this happens, you’ll need to be prepared to act swiftly to take physical possession of their hard drives the old fashioned way.

In the event you do not have the capability of replicating hard drives remotely, another approach

might be to ask your IT department to cause one or more of the suspects' phones or computers to malfunction. When the suspects call for assistance, you can make arrangements for IT personnel supporting the investigation to respond by taking the device to be "repaired." If they have administrative rights, they can unlock the devices and copy their contents. If not, they will need to collect relevant passwords so they can gain the access necessary to retrieve information from them.

Regardless of what approach you take, as an investigator, you should not leave any detail to chance or assume your IT guys know how to do this well. Instead, you should coach them through every aspect of what they will be doing and make sure you understand well the capabilities and limitations of the methodologies they will be using.

Step 2: Collect devices

Regardless of how sophisticated the cyber sleuths in your IT department might be in retrieving electronic information remotely, often times you will need to collect electronic devices from suspects and witnesses. However, as with other aspects of your investigation, you should not take anything for granted. Instead, it is essential that you carefully orchestrate this work to make sure it is done properly. Here are some recommendations from lessons learned in the school of hard knocks:

Take a complete inventory of the devices to be collected with all associated details: make, year, size of hard drives, software, type of connections required to interact with the devices, and any other relevant information. Get this wrong and you may have a device, but lack the means or know-how to copy its contents.

Develop a plan that will maximize your chances of taking suspects by surprise. Failure to do so will give the suspects time to cover their tracks by destroying the evidence. Make sure everyone on the team understands the plan and their role in carrying it out in advance of the day equipment is collected.

Ensure the IT professionals you recruit are competent. Interview every one of them, in the presence of an experienced cyber-investigator you trust, to ensure they are familiar with the equipment being collected and have the necessary skills and kit necessary to perform the work. Quiz them on their knowledge of device security features and whether they have the right connectors, software, and other gear necessary to pull data from the devices to be collected.

Develop and review with the IT team a detailed protocol for taking possession of the devices, obtaining and verifying passwords, putting devices into a mode where they cannot be "wiped" by the suspects, and replicating the data on them. For example, if you are collecting iPhones, the IT professionals must collect the pin to open the device and the suspects' "Apple ID password." These should be verified at the time of device collection in the presence of the suspect. The IT professional should then immediately use the Apple ID password to turn off the "Find My Phone" feature and put the device into "Airplane Mode." Otherwise, the suspect could remotely wipe the phone of all its data by connecting to their Apple account via another device.

Ensure you have sufficient numbers of IT professionals to perform the equipment collection. If, for example, you planned on collecting three devices (phone, tablet, and personal computer) from four suspects at once, I would recommend you bring four IT professionals — one for each suspect — to collect the devices, maintain proper chain of custody, and perform the data capture. If you are short staffed, it is more likely mistakes will be made and the time required to capture all the data may exceed your expectations.

Step 3: Process the data

Once you have collected electronic equipment, you will need extract the information from them and search it for documents or communications of interest. However, often times the data sets are so large that you will need to perform automated searches. To do this effectively, you will need to work with internal or external IT resources to load the data into an indexed file for searching by keyword or using other relevant document attributes. If you've got a large data collection, this process may take some time, so make sure you understand the resources they will be bringing to bear in performing this work and their anticipated time to completion.

Once you have a collection of responsive documents, you must then conduct a secondary review. To be effective, this work must be done by people familiar with the case and who are trained and experienced investigators. Regardless of how sophisticated your filtering tools are, they are no substitute for an intelligent investigator who can recognize patterns and relationships, and follow leads that may be needles in an electronic haystack.

Regardless of whether you are computer savvy or not, do not make the mistake of trusting your IT professionals to handle this critical aspect of your investigation. Instead, as with any other aspect of the investigation, take charge and manage every detail to ensure it is done right.

Jim Nortz

Founder & President

Axiom Compliance & Ethics Solutions, LLC