COSMOS
Navigate the Compliance Universe

CEP Magazine - November 2019
Digital forensics: A vital component of internal investigations

By Melody Haase

Melody Haase (melody@4discovery.com) is project manager at digital forensics firm 4Discovery in Chicago, Illinois, USA.

- linkedin.com/in/melodyannhaase/

Today's organizations rely heavily on the use of electronic data to run their day-to-day operations. Employees frequently access and use computers, email accounts, file shares, customer databases, various cloud accounts, and other sources of electronically stored information (ESI). These sources of ESI often contain confidential and proprietary data that are core to an organization's competitive strategy. When dealing with legal and compliance issues, these sources of ESI also contain evidence that relates to a multitude of internal matters, such as Foreign Corrupt Practices Act compliance, financial and compliance audits, harassment, trade secret theft, and breach of fiduciary duty. Often, these matters are handled internally, even though there may be future regulatory and/or legal proceedings.

Organizations typically employ IT personnel to set up and manage corporate systems. Internal IT usually helps with items like system administration, securing and maintaining IT assets, and troubleshooting user issues. However, they are often not equipped with the right knowledge base or tools to handle ESI that contains evidence. Digital forensics experts have a different area of expertise and are able to capture information in a manner that can be used in legal proceedings.

Computer forensics is the "use of specialized techniques for recovery, authentication and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, and authentication of data by technical analysis or explanation of technical features of data and computer usage."[1] Digital forensics experts focus on preserving and analyzing data from a wide array of sources and are typically called upon to write affidavits and provide expert testimony about their findings. It is important for organizations to understand how ESI is stored and how the use of digital forensics can play a role in their investigation.

During any investigation, there is a fact-finding process that involves collecting information and evidence from relevant parties and systems. Forensic investigators can assist with this process by collaborating with other members of the investigative team to develop strategies and collect and analyze data related to the facts of the case. This process allows companies to save time, money, and effort by creating efficiencies throughout the investigation. To give examples of how digital forensics can be used to assist with investigations, this article will use examples from a fact pattern that examines what happens when an employee departs for a competitor and may have taken confidential corporate information with them.

First, review the rules of the road

In the modern workplace, there are a wide array of laws, regulations, policies, and procedures that govern the organization's practice. This includes how data should be collected, stored, and used as well as the responsibilities of individuals who use organizational assets. In some instances, employers are limited by law in

how they can collect and use certain types of electronic data. For example, the Illinois Right to Privacy in the Workplace Act contains a section governing a line of prohibited inquiries that employers can make regarding the online accounts of current and prospective employees.[2] Before beginning any investigation, it is important to ensure all applicable laws, regulations, and policies are followed to maintain the integrity of any evidence collected during the course of the investigation.