Digital Evidence Collection

Properly Mitigate Legal Risk!

Most bank risk assessments demonstrate a measurable amount of security and reputational risk in the vulnerabilities exposed to malicious users with legitimate internal access. For example, we may list "rogue employees" as a threat, and "violation of access management policy" as a vulnerability. This example threat/vulnerability pair tends to our concerns over those with root access going into places and seeing documents they aren't supposed to see.

Unfortunately, we rarely remember to account for the legal risk inherent in developing adequate documentation. We hope that we can make a good enough case on our own, or look for other ways to terminate the employee, in order to avoid messy litigation.

Ideally we would bring in a third party to collect evidence in a forensically sound manner. Until now, this seemed a bit difficult. How can we even find somebody with those capabilities in the short amount of time necessary to collect the evidence? And how much would we have to pay somebody to stop what they're doing and quickly come on-site to collect the evidence?

infotex has created a new service to address this very issue. We have made pre-arranged associate agreements with Digital Forensics Experts to analyze data, and we have trained key members of our staff to properly seize and secure evidence in a manner that will hold up in litigation.

Thorough Documentation and Reporting Procedure

An extremely important step in digital evidence collection is ensuring appropriate Chain of Custody, which refers to the chronological documentation of the seizure, custody, control, transfer, analysis, and disposition of evidence. Without a proper chain of custody, litigants can easily question the validity of your claim. Anybody who has received a report from **infotex** knows that one of our major strengths is appropriate and thorough documentation.

Let **infotex** help you with your Digital Evidence Collection!

How the Service Works

Because we already have technicians working 24x7 due to our managed services, we can easily work on a retainer basis to be available 24x7 for digital evidence collection. We have trained key members of our staff to use our evidence gathering kits in a quick, thorough manner. We have a process for properly authenticating requests to ensure that we have received appropriate authorization. We work on a retainer and charge a flat fee based on the number of incidents you hope not to experience in a year's time, as well as the size of your organization (in number of employees), which calculates into our own risk management formula. We have appropriate expertise, resources, and tools for write blocking, password cracking, traffic monitoring, e-mail collection, imaging, hash verification, and library storage.

All you do is call us and let us know when and where to show up, and we will arrive prepared to perform triage to identify, preserve, and collect evidence. If necessary, we have a direct line back to pre-arranged Digital Forensics Associates as well as Attorneys who can assist us in the "triage" process.

We then deliver a copy of the evidence to you with affidavits and a "hash" that authenticates the image. We keep a library copy in our safe deposit box. We are available to testify in depositions and/or court if necessary, and we can make our Forensics experts available for analysis.

Way too often individuals will try something that they would not attempt if they knew that not only could they get caught, but they would also be prosecuted. If you want to mitigate the legal risk of an Information Security Incident or an Information Technology Incident, talk to us about our Digital Evidence Retainer Program!