INCIDENT RESPONSE & DIGITAL FORENSICS

Even the most secure organization faces the risk of system or network compromise committed by a malicious inside or outside party. In the event of resource misuse, policy abuse, denial-of-service, or data breach, *Intekras* consultants can immediately be dispatched to investigate the circumstances behind the event and provide assistance in remediation. *Intekras* can help recover any data that a wrongdoer sought to erase or delete from a hard drive or server, retrieve key data buried in documents and memoranda, and organize data contained in disparate digital information sources.

Handling an information security incident requires careful treatment of evidence and thorough investigative protocols in order to comply with Federal Rules of Civil Procedure and their relation to mandated eDiscovery processes. *Intekras*'s skilled forensics experts can help with:

- Timely reaction and onsite availability for incident management
- Chain of custody tracking for all client supplied materials
- Drive mirroring, data analysis, log reconstruction and incident research
- Secure storage facility for all client materials

Our process follows industry best practice in digital forensics:

- Collection & Preservation: Seal Evidence Sources, Write Block, Collect Application Data, Collect Configuration Data, Collect Event Log Data, Collect Data Files, Collect Operating System Data, Collect Network Traffic Data
- Examination: Process Data Structures, Extract Data, Recover Unallocated Data
- Analysis: Text Analysis, Image Analysis, Video Analysis, Executable Analysis
- Reporting: Work Performed, Findings, Evidence

"...Intekras can provide immediate 'on-call' incident response by dispatching certified systems engineers, investigators, and digital forensics personnel..."

Intekras can provide immediate "on-call" incident response by dispatching certified systems engineers, investigators, and digital forensics personnel who are able to identify causes and sources of breaches; establish a Scope of Incident; initiate Breach Triage & Investigation; perform extensive computer/network forensics on all affected platform components; identify, isolate, and stabilize compromised systems/networks; initiate network/system/data recovery efforts, and provide Post-Mortem debriefs to management, legal counsel, and law enforcement.

Furthermore, on an as-needed basis, *Intekras* is able to work with in-house counsel and law enforcement to assist in the identification and prosecution of perpetrators, serve as expert witness, and assist in the implementation of counter-measures to reduce the risk of re-occurrence.