Deloitte.

Harnessing the power of technology

Using digital forensic techniques

2019

Forensic

Digital forensics is a multifaceted process that streamlines and simplifies discovery to uncover issues, as well as helps increase investigation, litigation, and regulatory readiness. It can include a number of steps affecting various stages of an investigation, including:

- Data collection and processing
- Maintaining a chain of custody records
- Hosting, review, and production of data
- Email analytics

Increasing urgency

Digital forensics involves the collection, recovery, preservation, and analysis of data from digital devices. Its purpose is two-fold: securing and safeguarding data or potential electronic evidence and providing the capability to search the preserved data as part of an investigation or litigation process (and if required, to subsequently present the data in a legally admissible manner to relevant authorities and/or courts).

Challenges/situations you might face

- Internal investigations: These include data breaches, intellectual property theft, other frauds committed using technology as a tool or a target
- Faced with an employee exit and/or misconduct
- Increased demand for regulatory and legal data requests, both in volume and complexity
- Having the full set of skills needed to get the work done is important, but finding and retaining staff is difficult and expensive
- E-discovery skills and associated technologies are not your organisation's core business, and investing in technology is considered an expense
- Certain procedures/processes need to be put in place to be adequately prepared for an investigation or regulatory request

An invaluable, timely tool

Quick, decisive action is often crucial to determining facts and protecting an organisation's interests, whether the impetus is a suspected fraud, whistleblower claim, lawsuit, or regulatory inquiry. Organisations can strengthen their ability to address a diverse array of risks by establishing digital forensics as a standard procedure early on, in an internal investigation, and ensuring it encompasses relevant data sources while avoiding potential pitfalls.

We can support you across the following areas:

I. Technology-driven investigations

Cyber forensic

Investigations related to cyber-crime and data breaches, such as business email compromise, ransomware, malware attacks, and network intrusion

Technology

Investigations related to complex technology networks, system overrides, and manipulations`

Exit management and data theft

Investigations that primarily involve insider data theft, which can be conducted as proactive assessments and on a reactive basis

Unpublished price sensitive information (UPSI)

Investigations that involve the assessment of electronic communications channels such as computers, mobile phones, and distribution lists to help assess points of exfiltration of UPSI

II. Electronic discovery (e-discovery) and data management services

Electronic discovery

Addresses the technological challenges related to complex investigations or cross-border disputes/litigation, by implementing a practical approach (supported by specialised technology and processes to help manage and analyse large volumes of structured/ unstructured data sets)

Data separation and segregation

Involves separating data using e-discovery tools and capabilities during large divestitures or at the end of a joint venture or outsourcing arrangement; the process includes identifying sensitive information and securely erasing data to align with contractual obligations

Data preservation

Involves preserving data and information, especially for organisations undergoing insolvency proceedings, to help prevent the loss of commercially sensitive data and intellectual property; this can also be useful during a merger/acquisition

Privacy assessments

Involves using e-discovery capabilities to assess an organisation's preparedness to comply with data protection rules and to tackle instances of breaches, in line with the General Data Protection Regulation, Personal Data Protection Bill, 2018, etc.

III. Forensic technology advisory

Digital forensic capability development

Involves providing advisory and assistance on establishing forensic technology capabilities

Cyber forensic readiness

Focuses on enabling a cyber-ready and resilient business, and involves working with organisations to assess their readiness to deal with a cyber-breach and/or threat

Data discovery readiness

Involves helping organisations assess their information governance processes, readiness to tackle potential litigation and fraud investigation(s), and/or respond to e-discovery obligations

Staffing solutions

Includes providing onsite, short- and/ or long-term trained forensic technology professionals to organisations in order to assist as first respondents in early case assessment activities and/ or augment organisations' in-house forensic capabilities to conduct end- to-end investigations

The Deloitte differentiator

Globally aligned, locally focused.

Our local professionals, along with a powerful global network of forensic specialists in more than 35 countries, use sophisticated technology, forensic technology laboratories, and consistent methodologies/training protocols. As a result, when you engage Deloitte in a multi-jurisdictional matter, you receive consistent service and deliverables regardless of where the work is performed.

Not only will you get the support of a team experienced in handling large, national (and international) investigations and litigations, but also have access to a unique pool of resources experienced in working with technology and possessing an investigative mindset.

Contact us

NIKHIL BEDI
Partner and Head – Forensic
Financial Advisory
Deloitte India
T: +91 22 6185 5130
E: nikhilbedi@deloitte.com

JAYANT SARAN
Partner – Forensic
Financial Advisory
Deloitte India
T: +91 124 669 5024
E: jsaran@deloitte.com

SACHIN YADAV
Partner – Forensic
Financial Advisory
Deloitte India
T: +91 22 6185 6177
E: sachyadav@deloitte.com

Deloitte.