Deloitte.

Data breach investigation services

Businesses, today, have moved from a paper-based environment to an almost entirely electronic one. While the advantages of operating in such an environment are undisputable, it is imperative that organizations understand and address the risks of such an environment.

Electronic business environments can fall prey to external threats, such as hackers gaining unauthorized access to confidential data, or internal threats such as employees misusing sensitive data and information (intentionally or otherwise).Such threats or data breach can be disastrous to organizations and, as reported by media in similar cases in the recent past, may result in monetary losses, irreparable damage to their reputation or business loss.

While it is difficult to anticipate or control external threats, it is relatively easy for organizations to control the extent of internal data breach. At times, organizations may try to control data breach through internal controls but according to Verizon's Data Breach Investigation report 2014 that is insufficient. The report highlighted that employees used several channels to misuse and transfer confidential information outside the organization including instant messaging platforms, e-mails, web mails, File Transfer Protocol (FTP) transfers, transfers through removable media like pen drives, optical drives, hard copy print outs, cameras and mobile phones. While data breaches cannot be prevented completely even with significant implementation of controls, it is important for organizations to investigate the root cause of data breach cases and plug the gaps.

Deloitte's Forensic professionals can help the clients to identify the data breach footprint, assess the extent of damage and recommend strategies to plug gaps in a controlled environment. The team can also help to investigate the motives, modus operandi and identify the perpetrators involved in data breach and Intellectual Property (IP) leakage.

Our key services

- **Data/ IP breach assessment** – aimed to determine whether the incident has occurred or not and the severity of the breach.
- **Data/ IP breach investigations** – aimed to identifying the modus operandi of data breach, perpetrators, loss due to breach and gaps in controls within the organization. It can help to recover evidence from electronic devices involved in the breach by using a combination of the following methods:
  - Forensic imaging and collection of e-mails and other artefacts including remote devices.
  - Forensic image processing, recovery and extraction of documents of potential interest to the investigation including deleted, encrypted or hidden documents.
  - Analysis of USB and other portable media devices.
  - Registry and Internet history analysis.
  - Analysis of user, application and system logs.

  The evidence that is gathered is shared with the client in the form of a report that can be used for taking action- legal or otherwise - against the perpetrators.
- **Data/ IP breach notification assistance** – Clients are, often, required to notify regulatory bodies and several internal stakeholders of data breach incidents. The Forensic team can support in preparing data breach related communications that comply with regulatory requirements.
- **Documentation support** is provided to record the remediation activities undertaken in the event of legal proceedings.
- **Sanitizing digital media for secure disposal** - Secure sanitization of storage media of computers, laptops and other digital devices, in addition to, stand alone storage media, conforming to US Department of Defense Standards.

What sets us apart?

- **Strong technical expertise and experience:** The Forensic team comprises of the industry's best computer hacking forensic investigators, certified fraud examiners, former law enforcement officials, digital forensics, data analytics, and system and network domain experts. These professionals help in identification, collection, processing and analysis of electronic data in a forensically sound manner, and can support with expert testimony, in case of legal requirements.
- **Robust forensic technology infrastructure**: Deloitte in India operates one of the largest computer forensic/ electronic discovery labs in Asia, in addition to operating forensic labs in major locations like Mumbai, Delhi and Bangalore. The focus is to use advanced tools and technology to collect, process, and analyze electronically stored information (ESI) for better forensic investigations.
- **Cutting edge tools and flexible delivery model:** With long standing partnerships with leading forensic tool providers, the team has access to the latest versions of the most advanced investigative tools (EnCase, FTK, Nuix, Relativity and several others). It thereby significantly reduces the duration of investigation. Additionally, our delivery model is flexible and can be swiftly ramped up in terms of resources to support large projects at a short notice, both virtually and onsite.

For more details on the data breach investigation services, please reach out to the contacts mentioned below.

Key contacts:
Rohit Mahajan
National Leader & Senior Director,
Forensic services
Tel: +91 22 6185 5180
E-mail: rmahajan@deloitte.com

Suprabhat NM
Director and Lead, Data Analytics
Forensic services
Tel: +91 22 6185 5214
E-mail: suprabhatnm@deloitte.com

Sebastian Edassery
Director and Lead, Computer Forensic
Forensic services
Tel: +91 80 6627 6157
E-mail: edasserys@deloitte.com