

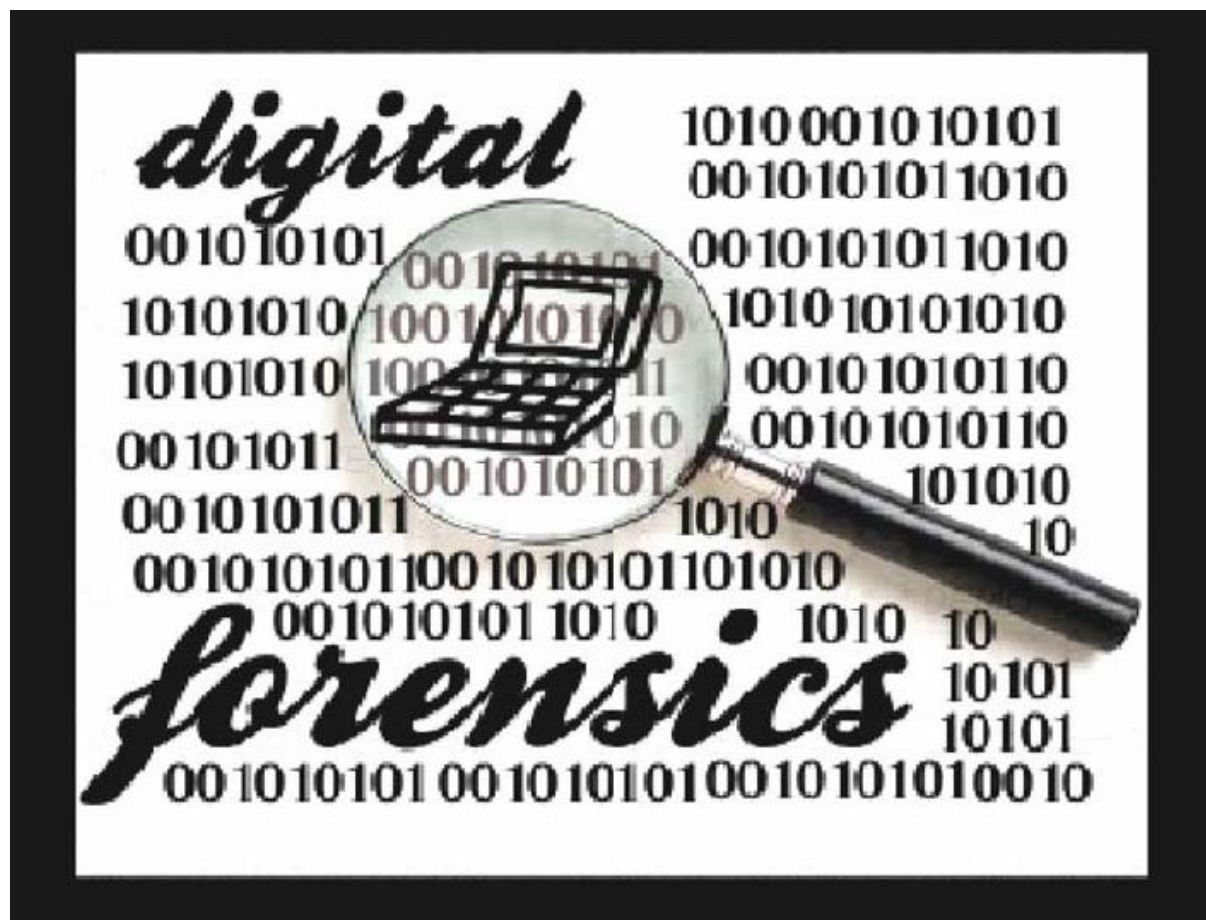
## **Combating Data Theft & Financial Fraud with Digital Forensics**

### **INTRODUCTION:**

In today's times, along with the development of the e-world, no doubt the world has come closer and transactions and dealings have become simpler; but the statistics pertaining to data theft – using identity switching and falsified identity too have risen conspicuously.

And since the e-world revolves virtually rather than physical involvement on the part of any person, it has become even tougher to fish out the miscreants; which brings into light the concept of digital forensics and the ways in which digital forensics help to combat the ever-speedily developing menace of the 21<sup>st</sup> century.

By involving the leading tools of Computer Forensics and a team of Experienced and Certified professionals we undertake the forensic analytical assignments for the benefit of not just business enterprises, but their clients and Law Firms as well. The team has total experience of handling Forensics of over 6000 Digital devices such as Desktops; Laptops; Servers; storage media etc.



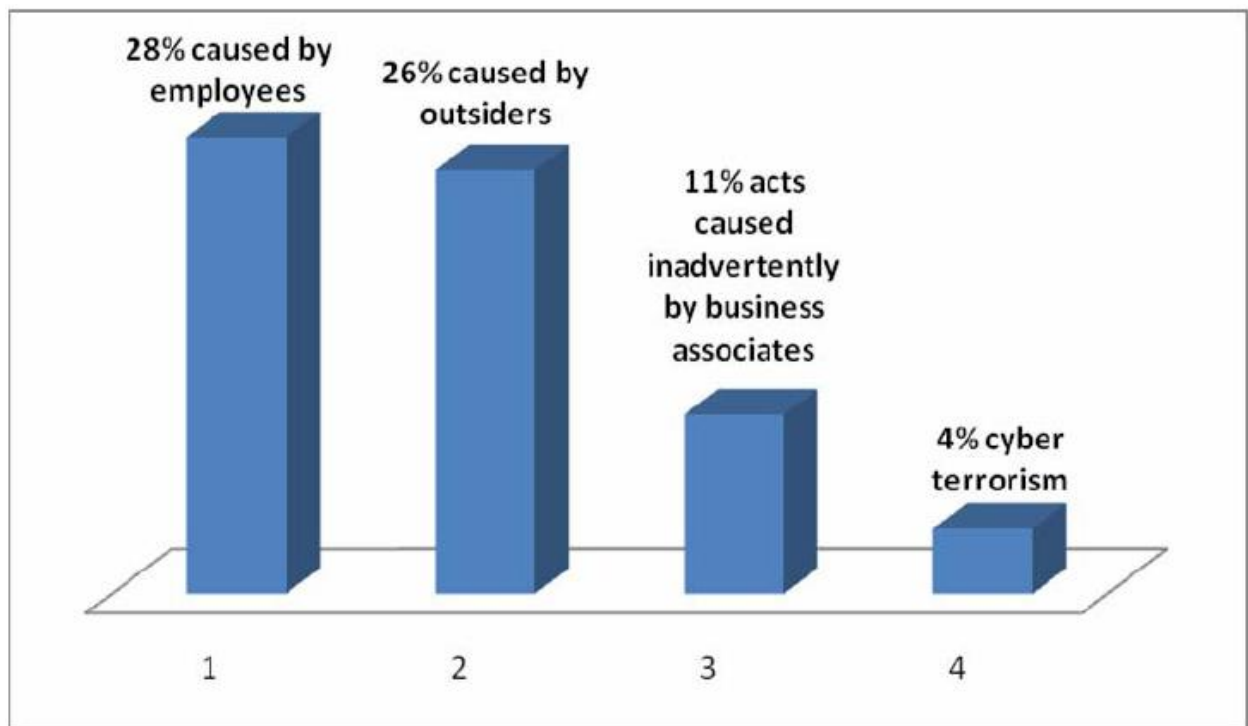
Given in detail below are relevant statistics along with pertinent case studies that would help put the point firmly across – the point as to why cyber forensics becomes a must as the usage and relevance of e-world gains an upper hand in almost every dealing and transaction:

### **STATISTICS:**

1. According to a survey conducted by Cert Co-ordination Center, nearly 90% of IT frauds occur because the vulnerabilities that are required to be patched are left unpatched; to put it simply, an overlook.
2. According to another recent survey conducted, India is ranked among the top five nations of the world in terms of security breaches ( KPMG India survey figures) – not exactly a record worth having, especially if we aspire to be ranked soon among the developed nations.

The following data listed below, will enable to understand the major causes of security breaches:

- 1. Caused by Employees [Disgruntled and Malicious Attacks]: 28%**
- 2. Caused by Outsiders [Malicious Attacks]: 26%**
- 3. Acts caused inadvertently by Business Associates: 11%**
- 4. Cyber Terrorism: 4%**



Furthermore, going by a month's IDS logs of a bank reflected that there are close to over 3200 intrusion attempts on their network, out of which over 70% were made from few IP addresses. Ironically, there could not be anything traced beyond the service provider of those IP addresses. (From Sify infrasecure.html).

Thus, the above example shows how important it has become to deploy both proactive & reactive cyber forensics – which in this case, is aided by Lab Systems (Pvt.) Ltd.

## **CASE-STUDIES:**

### **1. CASE-STUDY I:**

A top notch CEO (employee CEO) of a top notch corporate succeeded in convincing the Board about the utility of a few proprietary technologies to be imported which in turn would have – supposedly – enhanced the company's ability to be in the lead position in the market.

The Board after lot of discussions and deliberations approved the purchase of these technologies for a cost close to US \$ 2.5 Million.

The CEO who had obtained quotes from the overseas vendor decided to place a firm order with them and a 100 % advance payment was made to this vendor; few months past this placement, the said CEO left this corporate for better prospects.

Few months after the said CEO left, the Board realized that although the advance payment was made, no such technology was actually delivered and though, frequent requests to the overseas vendor were made, no proper response was made by the officials of the said technology vendor.

Finally after lot of efforts it was realized that this overseas vendor company did not exist and the CEO had duped his company of a whopping US \$2.5 M (roughly Rs 9.5 crores). It also became difficult to trace the present whereabouts of the CEO, not only because he changed all his personal contact numbers but also because he went abroad – to an unknown destination – for about 4 months.

Ultimately, after lot of internal discussions, the defrauded company decided to file a Complaint with the Crime Department of Police.

After tracking the CEO's Email and IP address from which he sent and received personal mail, his current home phone number and address was traced; after laying an elaborate trap he was eventually arrested too.

A thorough digital forensic analysis of the CEO's PC's and laptops seized at his home and doing the analysis of the deleted e-mails from his MS Outlook inbox, it came to be proved conclusively that the overseas company was indeed faked by him and that the bank a/c to which the amount was transferred belonged to his family members.

## 2. CASE-STUDY II:

A publicity and media major suddenly reported loss of critical data from their database; and thinking that this event was a one-off and could be an accident; they restored the lost data from a backup device and continued the operations. Three weeks later again, though, they lost another set of critical data and they took exactly same steps as in the first instance.

This company has a reasonably tight IT Security system including Firewalls and IDS etc however, the only difference was that they hardly bothered to check if all the available perimeter security devices worked well or not.

After the second incident they had one more incident within six days. That's when the top management decided to wake up and investigate further and after a lot of deliberation decided to get done a forensic analysis of all the three events.

Lab Systems with its rich experience in data theft forensics deployed their team and also interrogated the IT and the operations team of this publicity major. On thorough probing it was identified that in the past 3 to 4 months about 11 employees had resigned and were replaced by new persons.

Two of these ex-employees still had very easy access to the internal network of this company. They frequently intruded into the network at early morning hours and were taking over database administrator roles. After that they were involved in the cut & paste of critical data and were exporting that into a word document. This word document was emailed to some webmail accounts.

One of the employee's e-mail id was used as the company administrator had not disabled this ex-employee's mail id.

A thorough query using sophisticated e-mail forensic tools revealed the extent of collusion between a few current manager level employees and the two rogues who perpetrated this fraud.

The top management has subsequently filed an FIR with the local police office. Digital forensic evidence including logs of the IP addresses from where this incident occurred, e-mail relationship data and the word documents with all those critical data have been submitted to this Police agency so that necessary criminal action can be initiated.

An expense of more than US \$ 20,000 towards forensic analysis of the events led to protecting critical data of this company worth few million dollars.

In both the incidents mentioned, Lab Systems was the company majorly involved in fishing out the perpetrators; the firm's expertise proving very beneficial to flush out the felons.

## **Conclusion:**

With a team that has over 75 man years of experience; Lab Systems is a leading provider of products & professional forensic services right from cyber forensics to other fraud-management related services.

Over the years, Lab Systems India (Pvt) Ltd. has remained in tandem with the aspect of development – both in terms of science and technology and broadening the company's overall purview.

Maintaining the clients' trust and belief without compromising on the company's core values is something that Lab Systems takes pride on. Every issue is dealt with utmost professional delicateness keeping in mind the importance and relevance of such investigation and analysis.

One of the observations that we have made in our eight years experience in this field is that the perpetrators of crimes aforementioned actually sit inside the network itself having already crossed the network's firewall and IDS. The company's IT Security might end up assuming they are free from any risk after installing such secured perimeter devices but in actuality they are still not secure.

Hence keeping in mind about continued check-ups, our experts recommend that once a year, a forensic audit of all the systems needs be carried out to check if any malpractices are going on within the company. Prevention is better than cure, but if the ailment has already struck, it becomes very important to take in regular doses of necessary medications.

*Just as threats to **digital assets**—  
identities, intellectual property, theft of unclassified  
and classified data—  
keep rising to a new level, so too must  
investments in the ability to investigate, expose and  
Remediate such risks and threats, an  
Ability called "**digital forensics**" should also go up.*

We look forward to working with your organization also to assist you in securing the Cyber space of your network.

Lab Systems can be contacted Email Id: [contact@labsystems.co.in](mailto:contact@labsystems.co.in)  
[www.labsystems.co.in](http://www.labsystems.co.in)