Data explosion and Internet penetration has resulted in organisations having access to various types of data, public or confidential, in real time or otherwise. Most of this data is communicated across the organisation via the internet and is susceptible to cyber attacks. Such attacks can cause potential interruption of business, loss of intellectual property and damage to the company’s reputation. It is therefore imperative that organisations have effective incident response frameworks to counter cyber attacks.

**What is Cyber Incident Response?**

Cyber incident response is a precise set of actions to handle any security breach in a timely manner. Some common breaches include:

- An employee involved in intellectual property theft and the firm being unaware of what data has been leaked by the employee
- Presence of Malware/Virus on the network that might leak confidential information to external parties
- A ‘Denial of Service’ attack that has rendered resources useless
- Any incident of hacking where the critical servers of the organisation have been compromised
- A Phishing attack
- Deletion of logs and the other critical information from the network.

A robust incident response plan involves stages such as pre-incident preparation, Digital Triage Forensic (DTF) and post incident response plan to prevent similar occurrences in future.
## Cyber Incident response framework

<table>
<thead>
<tr>
<th>Phase 1 Preparation</th>
<th>Phase 2 Identification</th>
<th>Phase 3 Containment</th>
<th>Phase 4 Eradication</th>
<th>Phase 5 Recovery</th>
<th>Phase 6 Wrap-up</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objectives</td>
<td>Get familiar with the process and technology</td>
<td>Determine the scope and parties involved</td>
<td>Minimise the effect on IT resource</td>
<td>Eliminate compromise artifacts</td>
<td>Restore system to normal operations</td>
</tr>
<tr>
<td>Process</td>
<td>Categorise and priorities &amp; risk • Asset &amp; Data • Teams &amp; Roles</td>
<td>First-Response Collection &amp; Correlation of logs</td>
<td>Isolate the threat</td>
<td>System hardening</td>
<td>Plan for continuity strategy</td>
</tr>
<tr>
<td>Actions</td>
<td>Incident Response team assembly</td>
<td>Determine notification/escalation processes to report incidents</td>
<td>Create a task list based containment plan</td>
<td>Develop rules for indicators of compromised</td>
<td>Restore data from last known good state</td>
</tr>
<tr>
<td></td>
<td>Incident Response team assembly</td>
<td>Gathering Volatile Information (eg, Memory, Process, Network)</td>
<td>Disconnect system from production</td>
<td>Controls creation, Security Baselines, Configuration Reviews, Patching</td>
<td>Test, monitor and validate Systems</td>
</tr>
<tr>
<td></td>
<td>Conduct Interviews</td>
<td>Remove Illegitimate Access</td>
<td>Incident Response plan and policy creation/revision</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Initial Incident Reports</td>
<td>Update firewall Policy</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Our team can help your organisation respond to suspected data breaches and assist you in taking measures to mitigate such incidents in future. Our incident response process is created in accordance with several internationally accepted frameworks and has been refined by practical experience.

We can help assess your organisation’s technical and business related vulnerabilities, help strategise security improvements in light of business needs, work to develop compliance programs, and assist the internal audit function. We are familiar with the potential operational, financial, and regulatory impact related to data breaches and can help create a response plan or proactively investigate such incidents.

**Experience in**

- Provide investigative support
- Help in evidence collection and analysis
- Perform control gap analysis and assist in remediation
- Offer expert witness testimony
- Assist as a liaison in law enforcement.
Domain knowledge:
Our associates possess diverse skills in digital forensics, incident response, malicious code analysis, data analytics, and network architecture.

Leading technology support:
Our forensic technology lab is among the largest private forensic labs in India and is equipped with the latest tools and technology required for Digital Forensic and Incident Response. We have a dedicated forensic technology practice that is enhanced by KPMG’s experience in forensic accounting and investigations to unearth the modus operandi behind cyber crime, fraud and other misconduct.

Experience executing large, complex and sensitive engagements:
We have successfully executed several of the largest, complex and sensitive engagements in India including many high profile cases in the public domain. Our team is well versed with the sensitivity, urgency and complexity associated with disruptive circumstances.

Select Credentials

<table>
<thead>
<tr>
<th>Incident type</th>
<th>Select engagement details</th>
<th>KPMG assistance</th>
<th>Engagement Outcome</th>
</tr>
</thead>
</table>
| Cyber Identity Theft | A major public telecommunications company reported an incident involving possible identity theft. | • Identification of the root cause of the incident  
• Review and analyse the methods of operation of the perpetrator  
• Implementation of appropriate measures has been taken to avoid future risk  
• Further analysis of the malware in sandbox environment and analysis of audit logs revealed the attack used a known Trojan. | Client deployed appropriate cyber security controls and incident management procedures to handle such incidents in future. |
| Malware Attack | The electronic transaction system of a foreign commercial bank with operations in India was compromised by an attacker who performed unauthorised NEFT and RTGS transactions. | • Investigation of the process followed to perform the unauthorised transactions attempted  
• Web server log analysis, forensic acquisition and malware analysis performed to identify systems compromised  
• Detailed reverse engineering of digital foot prints of Trojan revealed the attack was initiated by an insider. | Insider attack was identified. Further action against employee taken by the client. |
| Data Leakage | Sensitive information such as employee appraisal data of a leading architectural service was circulated by an employee on personal email. | • Cyber forensic analysis of the perpetrator’s modus operandi to assess the e-mail trail  
• Forensic analysis revealed that the alleged employee had logged into the e-mail account of a senior member using web portal while carving of artifacts further showed anti-forensic activities. | Internal perpetrator identified. Further action against employee taken by the client. |
| E-mail Spoofing | Customers of a fortune 500 company reported emails received instructing transfer of outstanding payments to certain bank accounts across the globe. | • Investigation revealed involvement of an insider where the e-mails were traced to a domain that were registered by a competitor  
• Analysis of internet artifact revealed all domains were registered and used by the competitor to send these spoofed email. | Client sought legal action against the perpetrator. |
| Hacking | A major telecom company faced defacement of its web portal | • Preservation and collection of identified digital devices  
• Log analysis of more than 40 million line items to identify the locations from where attack originated  
• Identification of the modus operandi of the attack by perpetrators  
• Identification of control gaps to prevent recurrence. | The matter is sub-judice |
<table>
<thead>
<tr>
<th>Incident type</th>
<th>Select engagement details</th>
<th>KPMG assistance</th>
<th>Engagement Outcome</th>
</tr>
</thead>
</table>
| Intellectual Property Theft   | Theft of chemical formulations at a leading Indian firms operating in the Chemicals sector | • Assistance in identifying the intellectual property that was stolen by the identified perpetrator  
• Rebuilding the deleted web cache pages to identify data that was sent to personal email accounts 
• Mobile forensic for identifying the evidence related to Intellectual Property theft. | The client obtained an injunction from the court against the perpetrator                               |
| Destruction of data and evidence | Assisting a leading media firm in an internal investigation                                | • Forensic procedures/methodology for data collection 
• Recovery of deleted partitions and deleted files 
• Analysis of files/emails for identifying evidence of financial fraud 
• Identification of files for the potential evidence pointing to intellectual property theft. | Client sought legal action against the perpetrator                                                   |
| Digital document forgery       | Forgery investigation for a leading wines and spirits manufacturing firm                   | • Identification of digital documents which were used by the perpetrator for committing forgery 
• Email server log analysis to identify potential evidence 
• Hard drive analysis to recover deleted content and attempt to look for potential evidence. | • Client sought legal action against the perpetrator                                                 |
| Denial of service attack       | Web server crash at a leading financial institution                                        | • Event correlation by examining system and network logs and subsequent interviews of vendors, employees, and contractors 
• Analysis of firewall, intrusion detection system and performance management system logs for any outside attack 
• Database changes and modifications for any intended malicious changes to the financial systems. | • Sequence of events leading up to the incident was identified 
• Remedial action was taken to prevent future incidents.                                            |
| Social Engineering            | A large telecom operator in India faced unauthorised activity by a former employee         | • Relationship discovery to identify links and patterns in CDR data 
• Disk imaging and log analysis such as SSL and VPN, AD and GPRS 
• IP tracing and interviews to establish modus operandi for social engineering attack.            | The client conducted a review of operating procedures and systems                                    |
| Malware                       | Assisting a luxury retail firm in an internal investigation                                | • Analysis to identify espionage of intellectual property 
• Identification and analysis of key logger or any other malware which might be installed with the intent to leak IP to the competitor 
• Reverse engineer the identified executable file to study the nature and function performed. | The client considered appropriate action against the perpetrator                                    |