Cybercrime: investigation and intelligence services
The advent of technology has brought about a revolution in the way we live. Our communications, work, recreation, even utilities, have undergone a change and are being powered by technology, which is now faster, easier and more convenient than ever before.

However, just like brick and mortar institutions, the virtual environment has its own risks and challenges. The recent increase in cybercrimes has brought this threat to the attention of many organizations, which are now increasingly asking questions regarding the security aspects of this medium.

Today’s corporate world recognises the importance of external perceptions; that damage to an organization’s reputation is the greatest collateral damage it can face. This fear also stems from the fact that this can result in loss of revenue or destruction of shareholder value, even if it is not found guilty of a crime. There is also growing awareness that such threats are not just external. Insiders, including disgruntled employees, pose a much greater risk to a company, since they are harder to detect and guard against, compared to external threats.
Why bother about Cybercrime?

- Rise of underground web infrastructure (Dark Web)
- Media reports on recent incidents
- Penetration of technology (Personal and Official)
- EY Survey highlights data theft as #1 concern
- Insider threats
- Existing controls don’t deal with all unknown vulnerabilities
- Industry reports on increase in cyber attacks
Any crimes or acts committed against the confidentiality, integrity and availability of computer data or systems form the core of cybercrime. The most common ones are listed below:

1. Hacking and phishing
   - Hackers create fake water board website
   - Six arrested for online fraud
   - Former director of top college duped of INR 19 lakh in online fraud
   - Telecom executive detained for net banking fraud

2. Fraud
   - Cybercrime costs up to $500 billion to world economy
   - Four Indians charged with credit card fraud worth $200 million
   - Two Sri Lankans held for fake credit card fraud

3. Data theft
   - “India has 42 million cybercrimes every year...."
   - "...52 percent of such victims suffered attacks such as malware, viruses, hacking, scams, fraud and theft."
   - Companies lose INR 6 crore annually due to data breaches

4. Corporate espionage
   - "Banks will have to bear the cost of fraudulent card transactions through point of sales that do not have prescribed security features."

5. Denial of service

6. Cyber stalking

The newspapers are often peppered with tales of how the internet is used in crimes including fraud, and data and financial theft.
The next question that comes to mind is – who does it impact? And the honest answer is you. Whether you are part of a company handling data or an individual using technology for official use, you could be the target of cyber-criminals, and have probably been exposed to this already, directly or indirectly.

You just don’t know it yet.

Experts believe that there are basically two types of computer systems – ones that have been compromised and those that will be compromised.
Type of fraud that pose biggest risk to the industry

- Theft of data and information, IP infringement: 20%
- Bribery and Corruption: 15%
- Vendor fraud, kickbacks: 13%
- Fraud committed by senior management: 12%
- Regulatory non-compliance: 10%
- Procurement fraud and favoritism: 09%
- Accounting fraud: 09%
- Money Laundering: 04%
- Management Conflict of interest: 03%
- Asset misappropriation: 03%
- Others: 02%

Source: India fraud survey 2012, conducted by EY
According to the Norton report 2013, the main victims of cybercrime are likely to be:

- Owners of mobile devices: 63%
- Users of social networks: 63%
- Users of public or unsecured Wi-Fi: 68%
- Parents of children aged 8-17: 65%
- Users in emerging markets: 68%

Source: Technology fraud: a study by EY's forensic technology and discovery services team
According to the Internet Security Threat Report 2013, issued by Symantec, recent trends indicate the following:

- **Small businesses the most vulnerable to attackers:** Around 50% of targeted attacks were aimed at businesses with fewer than 2,500 employees. The largest growth area for such attacks are businesses with fewer than 250 employees and 31% of all attacks target them.

- **Malware authors acting as Big Brother:** Around 50% of mobile malware created last year attempted to steal information or track movements. The ultimate goal is to make money and learn people’s bank-related information, their phone numbers, the email addresses of their friends and business associates, their personal information, and even how to assume their identity by stealing it.

- **Vulnerability not the issue with mobiles:** As expected, the amount of mobile malware continues to rise. The past year saw a 58% increase in mobile malware families, compared to the previous one. With a 32% growth in vulnerabilities reported in mobile operating systems, it is tempting to put all the blame on this phenomenon. However, this would be wrong. Today, mobile vulnerability has little or no correlation to mobile malware.

- **Zero-day vulnerabilities available when attackers need them:** Zero-day vulnerabilities continue to increase, with 14 being reported in the past year. Attackers use as many zero-day vulnerabilities as they need, not as many as they have.

### The parallel universe of cybercrime – Dark Web

The concept of the Dark Web is fast gaining in importance. The Dark Web, also known as the Deep Web, Invisible Web and Dark Net, comprises web pages and data that are beyond the reach of search engines. Some of what makes up the Deep Web includes abandoned and inactive web pages, but the bulk of data that lies within has been crafted to deliberately avoid detection in order to remain anonymous. It is the hidden side of the internet that allows users to chat online, share files, or read or set up a website with almost complete anonymity. This allows cyber-criminals to surf protected websites and services without leaving tell-tale tracks.
Banking and financial institutions
- Internet banking fraud: Money being transferred out of banks from compromised customers' accounts
- Credit card fraud: Credit card information captured fraudulently being used for shopping
- Exposure of customers' confidential and private information leading to reputational risk

Automotive
- Theft of engineering designs through cybercrime
- Inadvertent leakage of data via JV partnerships

BPO/Knowledge-based companies
- IP infringement: Possibility of unauthorized access to IP-related data resulting in a massive loss in potential sales
- Exposure of clients' confidential information, which may expose it to reputational risk
- Exposure of contract terms and internal policies

Pharmaceuticals
- Confidential product formulation and FDA approval details
- Alteration (deletion/modification/removal/transference) of data
- Exposure of internal test results and R&D reports, especially related to clinical trials

Consumer products
- Theft of research and marketing data
- Counterfeiting and piracy
## Industry specific risks (cont'd.)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Risks</th>
</tr>
</thead>
</table>
| **Telecom** | • Denial of service  
               • Exposure of clients' confidential information, which may include financial details  
               • IP details of large clients, which may then be used to attack them |
| **ITeS**   | • IP infringement: Possibility of source codes of key products being compromised and shared with competition. e.g., in the BrainVisa case  
               • Exposure of clients' confidential information, which may include financial details of their customers  
               • Easy replication of source code to release crack versions in the market |
| **Real estate** | • Client-specific data, including personal, demographic, banking and loan details  
                        • Regulatory and government permissions including status and reasons for delay/denial (if any)  
                        • Details of property valuations, land holding status, actual cost of construction and profit statements |
| **Insurance** | • False claims and ID theft  
                      • Theft or leakage of internal data including "risk modelling" data |
Any organization looking to counter cybercrime should adopt the following multi-pronged approach

**Preventive measures**
- Carrying out risk assessments and identifying, implementing and continuously assessing controls and countermeasures required to mitigate vulnerabilities
- Formulating and deploying comprehensive policies that cover network, device, physical, data privacy, social media security, etc.
- Providing proactive and ongoing education and training
- Setting up cyber ‘intelligence teams’

**Detective measures**
- Identify key cyber threats related to business and IT systems
- Conduct forensic analysis to identify possible attacks that were successful/unsuccessful
- Establish possible scenarios/modus operandi
- Conduct tests to identify possible control lapses
- Suggest process/technological improvements and trainings

**Response measures**
- Quarantine affected systems and devices
- Conduct forensic evidence recovery from computers and devices
- Extract relevant data and conduct analysis
- Establish the modus operandi used for the crime and help the company plug the loopholes discovered
- Identify technical and human resources deployed to execute the internal or external cybercrime incident

**We can help companies identify whether their systems have already been compromised by cyber-criminals, and if so, guide them on answering key questions – how, who, when and what?**

**In the event of an incident, we can help companies achieve the following:**
Case 1

Client

A securities and brokerage company

Context

- The CEO got information that his company’s top customers were planning to move their business to a rival company, recently launched by some of its ex-employees. He was astounded to find that the new company was using his company’s research and proprietary intellectual property to capture his clients.
- Realizing that he had been a victim of data theft, data tampering and IP theft, he requested EY to help him understand the how and when of this action and get his property back.

Findings

- We identified evidence around unauthorized data copying and communications between suspected employees.
- During interviews with the company, these employees confessed to leaking sensitive data.

Our approach

- A review of user violation against company policy was carried out, including but not limited to, scanning of IT landscape (desktops, laptops, file servers, email and smartphone email servers and network).
- EY conducted forensic disk imaging of suspected host machines and analyzed the data to identify unauthorized user behavior, including deleted files, usage and browsing history.
- EY also conducted fact-finding interviews with existing employees, who were suspected of working with the ex-employees, who turned out to be part of the key development team.
Case 2

A digital media and content company

Context

- The IT and content management head of the company woke up in the early hours of a holiday to an email from his channel partner, a large online video content aggregator, informing him that the password change for his channel’s account has been successful. On resetting the password and gaining access to the channel account, he checked its contents. He was shocked to discover that 25 of the company’s most popular videos, which were also their highest revenue earners, had been deleted.
- He brought in EY to help him identify how this was done and who did this.

Our approach

- EY identified the series of events that had led up to the deletion, which included an unauthorized password change being carried out on two separate instances in the past.
- Using non-intrusive and non-disrupting forensic tools, the EY team collected key information over the network, to review and analyze it for exceptions.
- The team reviewed the logs of network devices, the events logs of the server, security events, scheduled tasks, network configurations and the email logs of authorized users.
- It also examined mailbox access logs of the affected channel.
- Using the data collected, along with the timelines of each activity, the team was able to reconstruct the series of events that led to deletion of content.

Findings

- The change of password was affected through an internet browser, used on a mobile phone, making it difficult to get an accurate IP address. However, the EY team was able to identify the mobile phone, using the version of the internet browser used.
- The content deletion command was triggered remotely via the back-up server of the client, which was hosted by a web-hosting service provider. Tracking the IP used to access this web server, the team was able to pin-point the location of the user. This address was a match with that of an ex-employee, who had parted from the company almost a year ago on a bitter note.
- Using these data points, the team was able to identify the chain of incidents, the modus operandi and the perpetrator of the fraud.
Case 3

Client

A container shipping company

Context

- The company suspected that some employee is colluding with an external entity and modifying shipment details to evade scrutiny and fines.
- EY was requested to conduct a forensic analysis of various systems on the office floor and global applications to identify unauthorized and suspicious transactions.

Our approach

- EY team reviewed the logs and data from IT systems and analyzed millions of emails and matched them against system transactions.
- We identified a pattern of similar modifications being executed in previous shipments as well, which were not detected.
- Using the data collected, along with the timelines of each of the incidents, we were able to unearth the series of events along with the individual who was initiating these suspicious transactions.

Findings

- In the previous three identical instances, similar fields were modified for the same shipper.
- In all the instances, modifications were first observed in the file attachment sent by the same person from the customer service team.
- Using these data points, the team was able to identify the chain of incidents.
- It recommended that the company tracked its old shipments – to whom and how the shipments were released from the dock.
- The team also recommended that the company should keep track of this shipper. This helped it to manage its future shipments.
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from your efforts to achieve your company’s potential. Enhanced management of fraud risk and compliance is a critical business priority – whatever the industry sector. With our more than 2000 fraud investigation and dispute professionals around the world, we will assemble the right multi-disciplinary and culturally aligned team to work with you and your legal advisors. In addition, we will provide you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our global activities.

About EY’s Fraud Investigation & Dispute Services (FIDS):

Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from your efforts to achieve your company’s potential. Enhanced management of fraud risk and compliance is a critical business priority – whatever the industry sector. With our more than 2000 fraud investigation and dispute professionals around the world, we will assemble the right multi-disciplinary and culturally aligned team to work with you and your legal advisors. In addition, we will provide you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our global activities.
Deep competencies: Our FIDS team has specific domain knowledge along with wide industry experience.

Forensic technology: We use sophisticated tools and established forensic techniques to provide requisite services to address individual client challenges.

Global exposure: Our team members have been trained on international engagements and have had global exposure to fraud scenarios.

Market intelligence: We have dedicated field professionals, who are specifically experienced and trained in corporate intelligence, and are capable of conducting extensive market intelligence and background studies on various subjects, industries, companies and people.

Thought leadership: We serve a variety of leading clients, which gives us deep insight into a wide range of issues affecting our clients and business globally.

Qualified professionals: We have a qualified and experienced mix of chartered accountants, certified fraud examiners, lawyers, CIAs, CISAs, engineers, MBAs and forensic computer professionals.

For more information please contact:

**Arpinder Singh**  
Partner and Head - India and Emerging Markets  
Direct: +91 12 4443 0330  
Email: arpinder.singh@in.ey.com

**Mukul Shrivastava**  
Partner  
Direct: +91 22 6192 2777  
Email: mukul.shrivastava@in.ey.com

**Amit Jaju**  
Partner  
Direct: +91 22 6192 0232  
Email: amit.jaju@in.ey.com
Connect with us

Our services
Assurance, Tax, Transactions, Advisory
A comprehensive range of high-quality services to help you navigate your next phase of growth
Read more on ey.com/IN/en/Services

Sector focus
Centers of excellence for key sectors
Our sector practices helps ensure our work with you is tuned in to the realities of your industry
Read about our sector knowledge at ey.com/IN/en/Industries

Stay connected
Easy access to our knowledge publications. Any time.
www.ey.com/subscription-form
Webcasts and podcasts
http://webcast.ey.com/thoughtcenter/
Follow us @EY_India
Join the business network from EY

For more information, visit www.ey.com/in
Our offices

**Ahmedabad**
2nd floor, Shivalik Ishaan Near C.N. Vidhyalaya Ambawadi Ahmedabad - 380 015 Tel: + 91 79 6608 3800 Fax: + 91 79 6608 3900

**Bengaluru**
12th & 13th floor “UB City”, Canberra Block No.24 Vittal Mallya Road Bengaluru - 560 001 Tel: + 91 80 4027 5000 + 91 80 6727 5000 Fax: + 91 80 2210 6000 (12th floor) Fax: + 91 80 2224 0695 (13th floor)

1st Floor, Prestige Emerald No. 4, Madras Bank Road Lavelle Road Junction Bengaluru - 560 001 Tel: + 91 80 6727 5000 Fax: + 91 80 2222 4112

**Chandigarh**
1st Floor, SCO: 166-167 Sector 9-C, Madhya Marg Chandigarh - 160 009 Tel: + 91 172 671 7800 Fax: + 91 172 671 7888

**Chennai**
Tidel Park, 6th & 7th Floor A Block (Module 601,701-702) No.4, Rajiv Gandhi Salai, Taramani Chennai - 600113 Tel: + 91 44 6654 8100 Fax: + 91 44 2254 0120

**Hyderabad**
Oval Office, 18, iLabs Centre Hitech City, Madhapur Hyderabad - 500081 Tel: + 91 40 6736 2000 Fax: + 91 40 6736 2200

**Kochi**
9th Floor, ABAD Nucleus NH-49, Maradu PO Kochi - 682304 Tel: + 91 484 304 4000 Fax: + 91 484 270 5393

**Kolkata**
22 Camac Street 3rd floor, Block ‘C’ Kolkata - 700 016 Tel: + 91 33 6615 3400 Fax: + 91 33 2281 7750

**Mumbai**
14th Floor, The Ruby 29 Senapati Bapat Marg Dadar (W), Mumbai - 400028 Tel: + 91 022 6192 0000 Fax: + 91 022 6192 1000

5th Floor, Block B-2 Nirlon Knowledge Park Off. Western Express Highway Goregaon (E) Mumbai - 400 063 Tel: + 91 22 6192 0000 Fax: + 91 22 6192 3000

**NCR**
Golf View Corporate Tower B Near DLF Golf Course Sector 42 Gurgaon - 122002 Tel: + 91 124 464 4000 Fax: + 91 124 464 4050

6th floor, HT House 18-20 Kasturba Gandhi Marg New Delhi - 110 001 Tel: + 91 11 4363 3000 Fax: + 91 11 4363 3200

4th & 5th Floor, Plot No 2B, Tower 2, Sector 126, NOIDA 201 304 Gautam Budh Nagar, U.P. India Tel: + 91 120 671 7000 Fax: + 91 120 671 7171

**Pune**
C-401, 4th floor Panchshil Tech Park Yerwada (Near Don Bosco School) Pune - 411 006 Tel: + 91 20 6603 6000 Fax: + 91 20 6601 5900
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EY refers to the global organization, and/or one or more of the independent member firms of Ernst & Young Global Limited.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

© 2017 Ernst & Young LLP. Published in India. All Rights Reserved.