



Grant Thornton

An instinct for growth™

Insights on Fraud Mitigation

Managing cyber-crime risks

November 2014



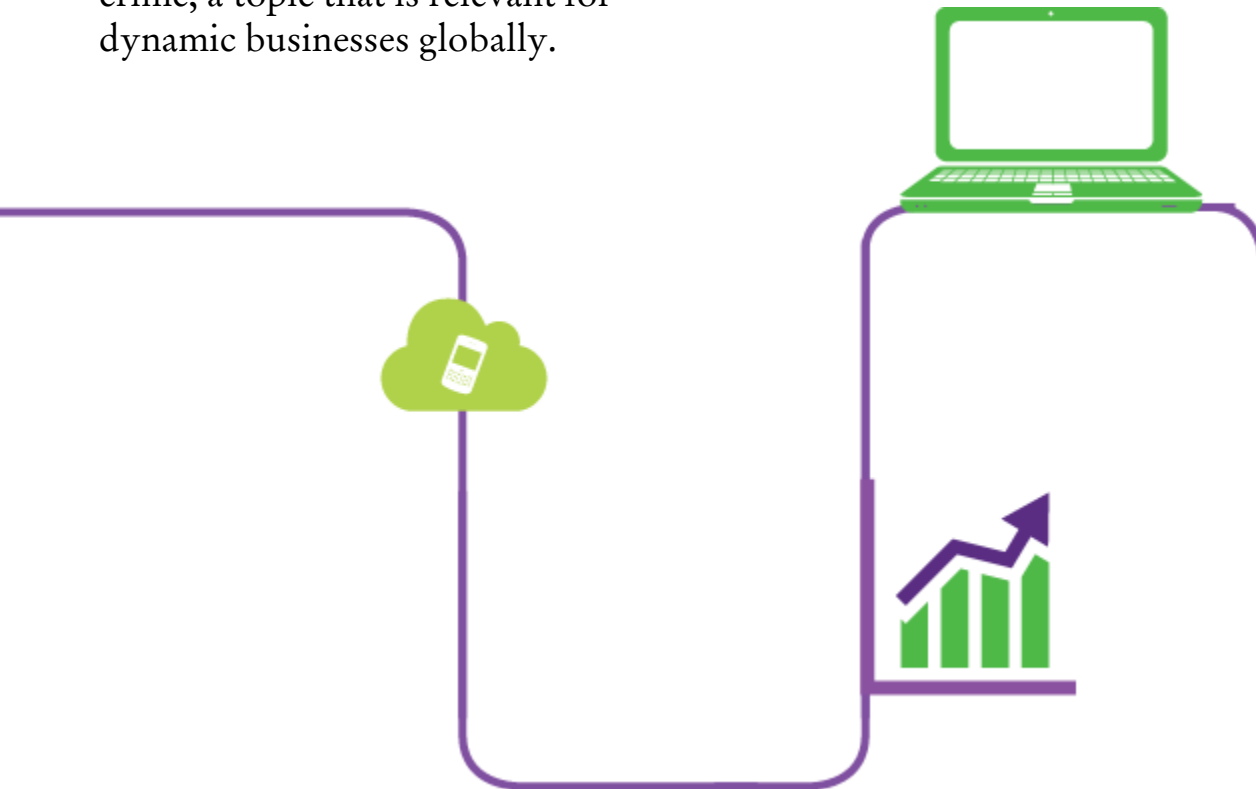
Welcome to the first edition of **Insights on Fraud Mitigation** - a periodic newsletter that is aimed at providing focused analysis, tips and tricks on dealing with the ever growing risk of fraud.

In this issue, we discuss cyber-crime, a topic that is relevant for dynamic businesses globally.

I am sure many of you have read about cyber-crime attacks on companies and the devastating effect it has on the company's operations.

The article highlights common cyber-crime threats and actions that companies can take to minimize the impact of cyber-crime.

We, of course, look forward to hearing from you. Should you have any questions, concerns or suggestions for future topics, please feel free to write to us.



Vidya Rajarao
Partner and Leader
Forensic Services



Cyber fraud is as much an internal threat as it is an external one. Many companies acknowledge that cyber-attacks on their IT systems intend to compromise the system for intellectual property, financial information and other sensitive information belonging to the customer, or other business partners of the company. Further, companies acknowledge that they are more concerned about cyber-crime perpetrated by employees or contractors as compared to hackers. Some of the most common cyber related risks faced by the companies are:

Cyber-attacks, which involve hacking, Denial of Services (DoS), Distributed Denial of Service (DDoS) or cyber extortion are in the form of a malicious code that gets implanted / injected into the IT network of a company.

1



Data breach involves access to information assets or critical data sets sensitive to the company.

2

The objective may be to steal sensitive and confidential information for financial gain, siphon money from customer accounts or simply disrupt services especially during peak periods with consequent loss of revenue to the company. Some of the instances to watch out for are:



- a disgruntled contractor gets hold of confidential information (such as bank account details, pay, bonuses and other rewards) and uses this information for personal advantage
- an employee obtains or has access to the accounts payable department and sets up dummy supplier information. Through this, fraudulent payments are made
- an employee shares sensitive information with their friends or connections on social media
- websites are defaced or disrupted by an attack on the server of the computer network so the server does not perform properly or prevents legitimate website visitors from accessing the site
- people are tricked into disclosing their confidential information via a fake email requesting confirmation of their password. There can also be a fake website which looks authentic and requests personal information. Using this information, it is possible to fraudulently transfer money from an individual's account
- an individual deliberately enters malicious software (for example viruses or trojans) into a computer network to steal information i.e., design, proprietary R&D, price lists and other confidential information.

Managing cyber-crime risks

Companies should implement a holistic approach to cyber protection. Such an approach should continuously prepare for and respond to potential threats and remediate breach risks. It should also take into account the lifecycle of information handled by employees, vendors, and consumers and should be sufficiently flexible to allow upgrades without placing a significant burden on end users.

Effective security coupled with rapid detection and investigation is critical to ensure that the impact of any breach or cyber-crime is contained to a manageable level.

Questions that companies can and should ask now to assess their cyber-readiness include:

1. Do we have a threat-based, asset-focused cyber security plan?
2. Is our Board and top management apprised of and aware of our cyber-security plan?
3. Do we know what our cyber security framework is protecting?

4. Can we explain the corporate cyber security initiative to our employees?
5. Do we have an integrated cyber security program?
6. How have we secured our information technology assets to imminent threats, both internal and external?
7. Are we prepared to respond in an event of an attack on our business eco-system?
8. Does our cyber security framework help in:
 - a) Maintaining data integrity
 - b) have a Quick Response Team including forensic technology specialists and legal counsels to minimise the impact of a cyber-attack
 - c) have an effective communication system
 - d) Disaster management
9. Do we conduct periodic cyber readiness assessments to protect critical data and IT assets?
10. Are we a forward looking organisation that incorporates critical aspects of cyber security framework to protect our business?

It is clear that cyber-crime risks will continue to increase as companies expand globally and use technology in innovative ways to deliver services to customers. It is imperative that companies understand cyber-crime risks, undertake periodic assessments and take immediate steps after an incident or breach so that they are adequately protected against such risks.



Upcoming Events

Annual ROXIN Alliance Meeting:

20-21 November 2014, Mumbai

Our experts are speaking at the event on the topic - Combating trafficking in counterfeit goods in South Asia.

Annual Conference on Internal Audit

21-22 November, Chennai

Our experts are speaking at the event organised by the Institute of Internal Auditors, Madras Chapter. The topic is Fraud & Investigation Changing Paradigm for Internal Audit.

Mitigating Financial Crime – Senior leadership symposium

25 November, Bengaluru
27 November, Mumbai

Grant Thornton in India is organising a two-city symposia that will help business leaders from financial services companies devise appropriate mitigation strategies.

Please register below to attend the sessions:

[Register for Bengaluru - 25 November 2014](#)

[Register for Mumbai - 27 November 2014](#)

Emerging Trends in International Arbitration

14 November 2014, Pune

The event will focus on a host of complex issues that come up during international arbitration such as evidence, discovery, and damages.

Click [here](#) to know more about our upcoming events.



Contact Us

For any additional information, please contact our subject matter experts:

Vidya Rajarao

Bengaluru

E vidya.rajarao@in.gt.com

M +91 99004 59932

Anil Roy

Gurgaon

E anil.roy@in.gt.com

M +91 98101 84474

Kunal Gupta

Gurgaon

E kunal.gupta@in.gt.com

M +91 95600 52733

Amit Shah

Mumbai

E amit.shah@in.gt.com

M +91 99303 66672

About Grant Thornton in India

Grant Thornton in India is one of the largest assurance, tax, and advisory firms in India. With over **2,000 professional staff across 13 offices**, the firm provides robust compliance services and growth navigation solutions on complex business and financial matters through focused practice groups. The firm has extensive experience across a range of industries, market segments, and geographical corridors. It is on a fast-track to becoming the best **growth advisor to dynamic Indian businesses with global ambitions**. With shorter decision-making chains, more senior personnel involvement, and empowered client service teams, the firm is able to operate in a coordinated way and respond with agility.

Over the years, Grant Thornton in India has added lateral talent across service lines and has developed a host of specialist services such as Corporate Finance, Governance, Risk & Operations, and Forensic & Investigation. The firm's strong Subject Matter Expertise (SME) focus not only enhances the reach but also helps deliver bespoke solutions tailored to the needs of its clients.



Our offices

NEW DELHI

National Office
Outer Circle
L 41 Connaught Circus
New Delhi 110 001
T +91 11 4278 7070

CHENNAI

Arihant Nitco Park, 6th floor
No.90, Dr. Radhakrishnan Salai
Mylapore
Chennai 600 004
T +91 44 4294 0000

KOLKATA

10C Hungerford Street
5th floor
Kolkata 700 017
T +91 33 4050 8000

NOIDA

Plot No. 19A, 7th Floor
Sector – 16A,
Noida – 201301
T +91 120 7109001

AHMEDABAD

BSQUARE Managed Offices,
7th Floor, Shree Krishna Center,
Above Crossword,
Nr. Mithakali Six Roads,
Navrangpura,
Ahmedabad 380009
T - +91 9825 073080

GURGAON

21st floor, DLF Square
Jacaranda Marg
DLF Phase II
Gurgaon 122 002
T +91 124 462 8000

MUMBAI

16th floor, Tower II
Indiabulls Finance Centre
SB Marg, Elphinstone (W)
Mumbai 400 013
T +91 22 6626 2600

PUNE

401 Century Arcade
Naranghi Baug Road
Off Boat Club Road
Pune 411 001
T +91 20 4105 7000

BENGALURU

“Wings”, 1st floor
16/1 Cambridge Road
Ulsoor
Bengaluru 560 008
T +91 80 4243 0700

HYDERABAD

7th floor, Block III
White House
Kundan Bagh, Begumpet
Hyderabad 500 016
T +91 40 6630 8200

MUMBAI

9th Floor, Classic Pentagon,
Nr Bisleri, Western Express Highway, Andheri (E)
Mumbai 400 099
T +91 22 6626 2600

CHANDIGARH

SCO 17
2nd floor
Sector 17 E
Chandigarh 160 017
T +91 172 4338 000

KOCHI

7th Floor, Modayil Centre
point, Warriam road junction,
M.G.Road,
Kochi 682016
T +91 9901755773

Grant Thornton India LLP (formerly Grant Thornton India) is registered with limited liability with identity number AAA-7677 and its registered office at L-41 Connaught Circus, New Delhi, 110001

Grant Thornton India LLP is a member firm within Grant Thornton International Ltd ('Grant Thornton International').

Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered by the member firms independently.

For more information or for any queries, write to us at contact@in.gt.com

www.grantthornton.in