# Forensic Focus

**Vidya Rajarao**
*Leader, Forensic Services*
*Bangalore, India*

Welcome to the fifth edition of Forensic Focus. This newsletter is designed to harness the knowledge of economic crime and disputes, in India and worldwide.

I am pleased to announce that from this edition onwards, we will cover one particular topic of interest for the reading convenience and interest of our readers. In this edition we will discuss the growing threat of cyber crime attacks and what organisations can do to mitigate threat from the cyber world.

Please save the date for our events as listed in our upcoming events section.

To read more about various fraud control methodologies and our upcoming events, please register and visit our Fraud Academy at *http://fraudacademy.pwc.co.in*

As always, we hope that you will find this edition of interest and welcome your feedback and suggestions for future topics.

Please feel free to contact me at *+91 (80) 4079 7002* or at *vidya.rajarao@in.pwc.com*

# Introduction

The last decade has seen an unperturbed growth in the use of internet, introduction of advanced technology handheld devices and sophistication of consumers in the use of e-commerce. Among several advantages of convenience and sophistication, companies are exposed to a host of cyber threats which may manifest into an Achilles' heel.

Cyber crime like any other economic crime is motivated by financial gain or economic espionage. Companies may be vulnerable to notorious hackers who would sell compromised customer information or competitors looking to steal sensitive market insight to gain competitive advantage. Regardless of the motive, the question here is whether the systems and cyber security infrastructure are being compromised in your organisation?

As technology advances, cyber threats are also becoming highly complex, and continually evolving. For these reasons, companies need to embrace a philosophy that recognises the realities of today's cyber threats and protect their businesses accordingly.

## Defining Cyber Crime

An economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming[1], and stealing personal information like bank account details. It's only a cyber crime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one[2].

## Cyber crime landscape in India

In 2008, Indian companies in the financial services sector, IT/ITes and BPO/KPO sector were toying with the idea of opting for cyber crime insurance owing to increased incidences of cyber crime[3]. This magnifies the issue of cyber crime and how companies understand the gravity of the situation.

According the National Crime Bureau, 966 cyber crime cases were registered under the Information Technology (IT) Act, 2000, in 2010 as against 420 in 2009. Karnataka reported highest number of cases (153), owing to heavy concentration of IT/ITes and BPO companies in the state, followed by Kerala (148), Maharashtra (142), Andhra Pradesh (105), Rajasthan and Punjab (52 each). Under the Indian Penal Code (IPC), 356 cyber crime cases were registered in 2010 as against 276 cases in 2009. Maharashtra reported the maximum number of such cases (104), followed by Andhra Pradesh (66) and Chhattisgarh (46)[4]. Statistics for the number and types of organisations affected by cyber crime is unavailable as many organisations fear to report cyber crime cases owing to damage to brand and reputation. The numbers reported being low does not mean that cyber space has become more secure and organisations are more vigilant. Regardless of an organisation's perception of the strength of its controls, it should consider performing tailored forensic analysis procedures on the network and key servers to point out indicators of security breach. It is important for organisations to bear in mind that timely check of commercial softwares such as virus protection and intrusion detection systems is of prime importance to strengthen the cyber security programme.

[1] *"As defined in the Global Economic Crime Survey 2011 by PwC: Phishing is an email fraud method in which the fraudster sends out legitimate looking emails in an attempt to gather personal and financial information and Pharming refers to the redirection of website traffic by hackers, with the aim of obtaining personal and financial information.*

[2] *As defined in the Global Economic Crime Survey 2011 by PwC in conjunction with our survey academic partner, Professor Peter Sommer*

[3] *http://www.financialexpress.com/news/firms-log-into-insurance-to-cut-cyber-crime-losses/348523/1*

[4] *http://www.livemint.com/2011/12/19005304/Cybercrime-on-the-rise-but-no.html*

# *Managing Cyber crime threats*

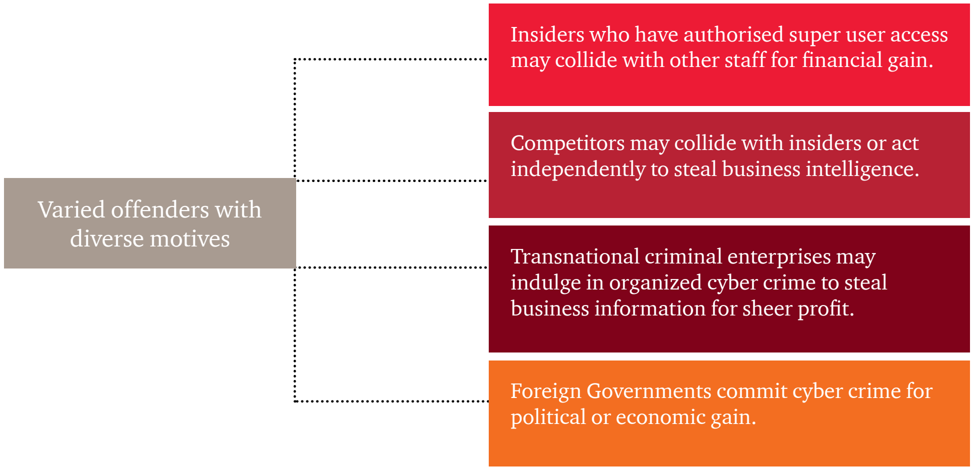
## Salient Features of a Cyber Security Programme - Vinay Nayak & Sujoy Mitra

Before we dive into the practical solutions for mitigating cyber crime risks, let's look into some of the key threats that may mar your organisation's reputation and brand.

Today's advanced cyber threats are two pronged: to steal targeted data, disrupt services and operational disruption or gain access for the purpose of misappropriating assets and to maintain access to the environment for as long as possible, thus enabling future intrusions. These threats apply to all industries, not just to those that deal with payment cards or personal information. Organisations that have proprietary data that is perceived to be of economic intelligence value or any organisation contemplating or already involved with international business transactions are likely targets as well as their external law firms.

An active but undetected cyber intrusion can include:

- Unauthorized web pages created on an Internet-facing web server;
- Outbound transmission of data over unknown and unauthorised ports;
- Large compressed files being transmitted outbound;
- Unusual connections between a user systems using native operating system networking features;
- Log entries on domain controllers capturing the execution of unauthorised programmes.



Varied offenders with diverse motives

Insiders who have authorised super user access may collide with other staff for financial gain.

Competitors may collide with insiders or act independently to steal business intelligence.

Transnational criminal enterprises may indulge in organized cyber crime to steal business information for sheer profit.

Foreign Governments commit cyber crime for political or economic gain.

## Cost of cyber attacks

Cyber attacks causing operational disruption to organisations and/or their business partners incur significant costs – both financial and non-financial. Some of the consequences have been listed below to enhance understanding of having a robust cyber security programme[5].

- Post a cyber attack, the organisation has to prepare an incidence response plan which includes a significant cost of remediation. This cost typically includes liability of stolen assets or economic intelligence, damaged cyber security system repair cost and importantly cost incurred in the form of incentives provided to business partners, customers and employees to maintain relationship and boost their confidence after the attack.
- As a part of the incidence response plan, organisations try to strengthen their cyber security which also comes at a cost. Following increased cyber security protection cost, there may also be certain organisational changes, recruitment or deployment of additional resources, training costs and cost of engaging consultants and third party experts.
- In case of theft of market insight information or any other sensitive data, the organisation may fail to attract consumers resulting in loss of revenue.
- It has been often seen that cyber attacks lead to litigation costs in addition to the reputation damage which adversely affects employee, investor and consumer confidence.

## Is your cyber security programme robust? - Characteristics of a robust cyber security programme

The two most important business issues or factors driving the information security spending of an organisation were cited as economic conditions and the need to ensure business continuity and disaster recovery by PwC's 2012 Global State of Information Security Survey.

There have been efforts globally to address this business risk. To cite one example, in October 2011, the U.S Securities and Exchange Commission (SEC) issued guidelines to public companies on disclosure regarding cyber security risks and cyber incidents. Through this document SEC has provided guidance to public companies to disclose their cyber security risks and vulnerabilities (which may materially affect an investor's decision) in their annual financial report.

Against this backdrop, in this article we would like to introduce salient features of a robust cyber security programme:

| Tone at the top | Risk & Impact based Analysis | Objectives of CIA | Embed cyber security programme | Monitoring & Review |
|---|---|---|---|---|
| 1. Management Buy in.<br>2. Top level commitment. | 1. Risk Factors.<br>2. Factor consequences of cyber attacks. | 1. Standard Operating Procedures (SOPs). | 1. Periodic trainings to staff.<br>2. Explain indicative red flags. | 1. Revisit SOPs annually.<br>2. Set incident response team.<br>3. Independent audits by third parties. |

[5] *http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm*

## Tone at the top

For any programme to function smoothly and effectively it is important to get a management buy-in and have the management involved. Entering the cyber environment represents a seismic shift in the security landscape for all organisations. It also highlights some of the structures, actions and capabilities that organisations can apply to achieve sustainable success in the cyber age. We believe that a cyber savvy CEO who understands the risks and opportunities of the cyber world will realise the benefits and manage the risks for his/her organisation (both private and public) more effectively. The tone at the top should view cyber crime as a business issue and not only an issue to be dealt by the Chief Technology Officer or the Chief Information Officer. The top management must be committed to take a tougher and clearer stance on cyber crime. While demonstrating top level commitment through, for instance a legal action, the organisation must also tactfully reveal information on their best practices and processes to avoid divulging insights to potential cyber intruders.

## Risk and Impact based Analysis

An organisation must conduct risk and impact based analysis for various threats and lay out a blue print of the counter measures that the organisation plans to adopt. While evaluating cyber security risk all relevant information including cyber attacks in the past (both specific to the company as well as relevant to the industry as a whole), frequency of those attacks and the severity of those attacks must be taken into account. An impact based analysis helps to identify the potential financial and non-financial damages due to cyber attacks and focus the organisation's efforts in the right direction.

A risk based analysis on the other hand helps to identify various areas within an organisation that are largely vulnerable to cyber attacks. A cyber programme also needs to align itself to the risk appetite of the company. Each internal control programme, and in this instance cyber security programme, has a cost associated with it and the organisation needs to do a judicious evaluation of the importance of each risk and the organisation's willingness to devote time and resources to help meet the objective of the programme.

## Meet the objectives of CIA (Confidentiality, Integrity and Availability)

CIA is commonly known in the IT security industry and stands for Confidentiality, Integrity and Availability. It is a widely used benchmark for evaluation of information systems security and the acronym is a benchmark of the overarching objectives that any IT Security programme needs to meet and is well applicable to a cyber security programme as well. CIA needs to be embedded into the risk and impact analysis so that the programme can proceed in the right direction. Set up and/or revisit Standard Operating Procedures (SOPs) and baseline for various system and internet related settings to meet the objectives of CIA.

## Embed cyber security programme

In order to embed and bear fruits of an effective cyber security programme, it is essential to raise awareness of cyber threats through periodic trainings to staff, conducting workshops to explain indicative red flags e.g. highlighting recent examples of cyber frauds, walking the staff through the means followed by the perpetrator and avoiding the pitfalls.

### Monitoring & Review

In order to maintain a robust cyber security programme, it is inevitable to be aware of the current and emerging cyber environment (Situational Awareness) – only then can the organisation make well-informed decisions and do the right things at the right time. Setting up a cyber incidence response team that can act and adapt quickly – the organisation can then track, risk-assess and deal with an incident as soon as it is spotted anywhere in the business. In addition, recruiting the right people with the relevant skills and experience who can pass their knowledge on to everyone else is helpful in mitigating the financial cost of an incident. It further helps to create a 'cyber-aware' organisation that can protect itself better. The incidence response team must revisit cyber security systems and protocols annually or more frequently based on the industry trends and the organisation's dependence on technology.

More often than not, periodic independent audits and reviews by third party who bring in an outsider's perspective on the robustness of the implementation of the programme turns out to be helpful.

## Conclusion

Managing cyber threats is the need of the hour in this fast paced business environment. There is no one-size-fits-all solution. Every cyber security programme must be bespoke and pragmatic and must spell out current trends and issues of the industry.

| ***Vinay Nayak***<br>*Manager*<br>*Forensics Practice* | ***Sujoy Mitra***<br>*Analyst*<br>*Forensics Practice* |
|---|---|
| Tel: +91 22 6689 1626 | Tel: +91 22 6689 1637 |
| Email: vinay.nayak@in.pwc.com | Email: sujoy.mitra@in.pwc.com |

# Upcoming events

## *Why cyber crime matters?*

Date | Friday, 17  February 2012
Location | My Fortune, Cathedral Road, Chennai

## *Addressing pressing issues in the Engineering & Construction Industry*

Date | March 2012
Location | Mumbai

For any queries, please contact Ms. Divya Rishi | Email: divya.rishi@in.pwc.com | Tel: +91 22 6689 1624 www.pwc.com/india

This publication does not constitute professional advice. The information in this publication has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this publication represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

AK 264 January 2012 Forensic Focus_Newsletter.indd

Designed by: PwC Brand and Communications, India