CMAI Association of India
Communication Multimedia
And Infrastructure

Powering Financial Solutions

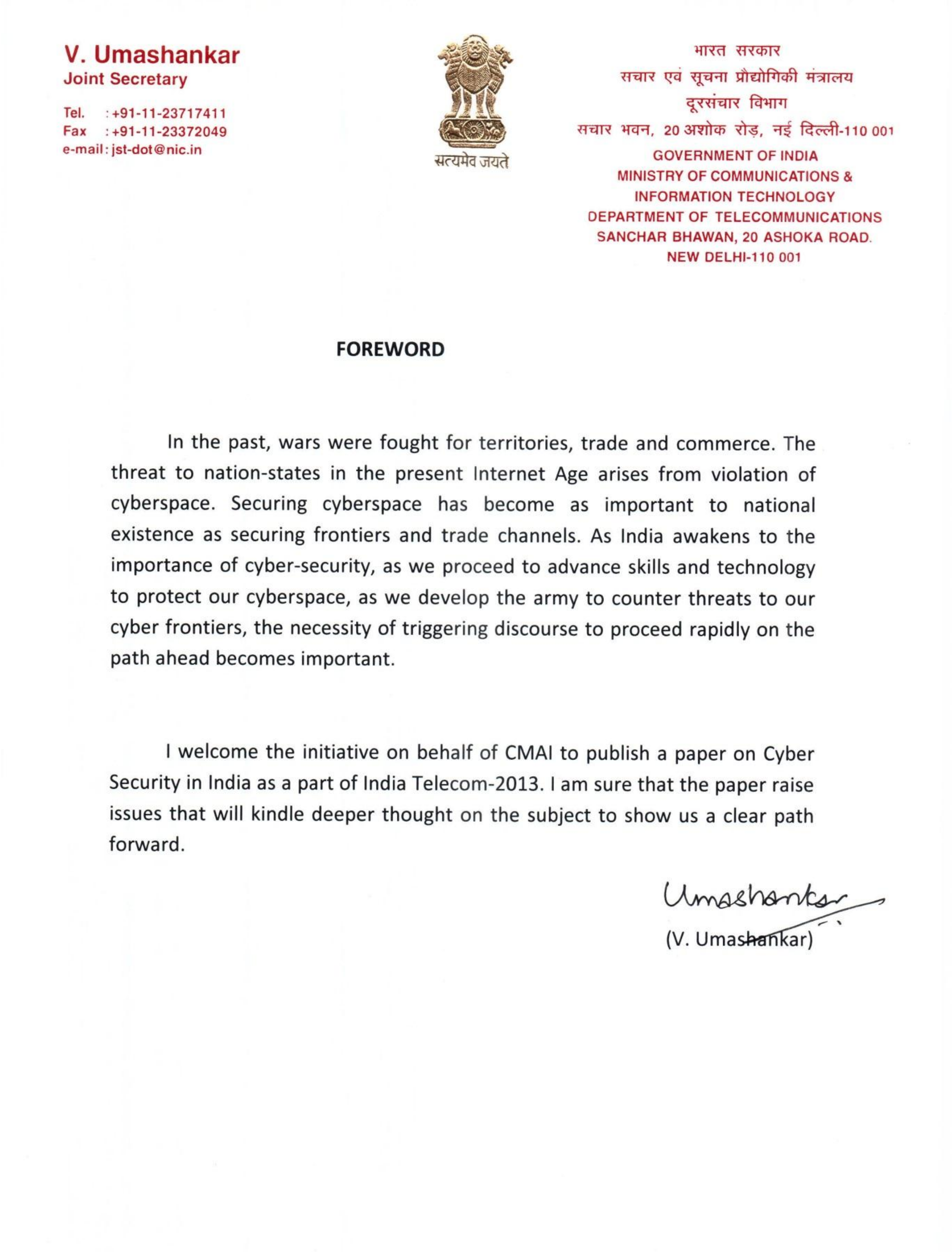
INDIA TELECOM 2013

White Paper

# Cyber Security in India:
## A Skill-Development Perspective

**Authored by:**
Ranjan Kumar | Niladri Mukherjee
Dion Global Solutions
Dec, 2013

www.dionglobal.com



**V. Umashankar**
**Joint Secretary**

Tel. : +91-11-23717411
Fax : +91-11-23372049
e-mail : jst-dot@nic.in

सत्यमेव जयते

भारत सरकार
सचार एवं सूचना प्रौद्योगिकी मंत्रालय
दूरसंचार विभाग
सचार भवन, 20 अशोक रोड़, नई दिल्ली-110 001
GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS &
INFORMATION TECHNOLOGY
DEPARTMENT OF TELECOMMUNICATIONS
SANCHAR BHAWAN, 20 ASHOKA ROAD.
NEW DELHI-110 001

## FOREWORD

In the past, wars were fought for territories, trade and commerce. The threat to nation-states in the present Internet Age arises from violation of cyberspace. Securing cyberspace has become as important to national existence as securing frontiers and trade channels. As India awakens to the importance of cyber-security, as we proceed to advance skills and technology to protect our cyberspace, as we develop the army to counter threats to our cyber frontiers, the necessity of triggering discourse to proceed rapidly on the path ahead becomes important.

I welcome the initiative on behalf of CMAI to publish a paper on Cyber Security in India as a part of India Telecom-2013. I am sure that the paper raise issues that will kindle deeper thought on the subject to show us a clear path forward.

Umashankar

(V. Umashankar)

## FOREWORD

The launch of this white paper represents another milestone in the continuing endeavor of CMAI to promote an action-oriented dialogue on critical issues in the ICT and Telecom sector. Cyber Security, the chosen theme of this white paper, has emerged to be a vital element of our safe and secure existence as a society, and as a nation.

Building cyber security skills in the country requires a framework within which multiple stakeholders can collaborate and develop an integrated response. CMAI is keen to drive forward an action-oriented agenda, as a partner and an enabler in this endeavor.

**NK Goyal,**
**President, CMAI**
http://www.cmai.asia/

On the occasion of India Telecom 2013, an event bringing together global participants in the Telecom and ICT sector, Dion has partnered with CMAI through this white paper to generate a vigorous dialogue between various stakeholders on cyber security skill development in the country.

As a global research and technology solutions provider, Dion interacts with decision-makers and policy planners at various levels. Leveraging rich insights from those interactions, its in-house research capabilities and inputs from cyber security experts, we have drafted this white paper.

Our sincere hope is that this document ignites farsighted thinking and active participation of all stakeholders in the arena of cyber security skill-building.

**Ranjan Kumar,**
**Vice President, Research and Analytics,**
**Dion Global Solutions**
http://www.dionglobal.com/

## Executive Summary and Acknowledgement

To repeat an oft-quoted cliché, India presents a study in stark contrast. We live in a socio-economic milieu where millions still go without food and shelter, even as more than 200 million of our citizens are zipping on the Internet autobahn at breakneck speed. And, at this pace, reaching 243 million users by June 2014, we are set to overtake the USA and have the world's second largest base of Internet users[1].

For the government and, for society at large, howsoever, incongruous the word 'Internet' sounds next to *roti* (food), *kapda* (clothing), *makaan* (shelter), the fact remains that the virtual world has become as much a reality of our existence as the physical one we inhabit. And, this coexistence does not operate in different silos. Instead, increasingly, the virtual or the cyber world is working in tandem with our bricks-and-mortar existence, and more significantly, altering it in multiple ways. Although, this is largely for better but, it is also quite often leading to drastic consequences.

Now, we realize that what happens in the Cyber world and its 'touch-points' with the physical world, have significant implications for our financial, personal and national well-being. And, this is only going to increase in magnitude. In this backdrop, Cyber Security is no longer an esoteric past-time activity in which geeks indulge, but has, and should become a mainstream concern for business and national leaders, and even individuals.

The question that arises is: Are we ready, as a nation, as a civil society, as a business, and as individuals to adopt and practice Cyber Security?

The Government of India has announced a new Cyber Policy 2013, under which 5 lakh cyber warriors will be trained in the next two years. This calls for an integrated approach requiring close collaboration between academia, educational

[1] *Internet and Mobile Association of India (IMAI)*

institutions, private sector, government agencies, cyber experts and most significantly, the national intelligence and defense establishment.

CMAI and Dion Global Solutions, after extensive research, have come out with this white paper, which analyses the skill-gaps in the domain of cyber security and various aspects of skill development. The paper examines the question from a skill development perspective for multiple stakeholders, and drawing upon the inspirational story of Israel which has emerged as the 'Go-To' destination for cyber security, provides a broad action plan framework that can guide us on the path to a 'Cyber Secure' nation.

We would like to acknowledge and thank the following people for their valuable contribution and inputs in preparing this white paper.

In alphabetical order:

**Mr. Akash Agarwal, Country Manager, EC Council**

**Mr. Gulshan Rai,** Director General, Indian Computer Emergency Response Team

**Mr. Saket Modi,** Ethical Hacker and CEO, Lucideus Tech

**Mr. Sanjay Bavisi,** President and Co-founder, International Council of E-commerce Consultants

**Mr. Vineet Kumar,** Chief Technology Officer, Jharkhand Police

# TABLE OF CONTENTS

## Cyber Security- A National Need?

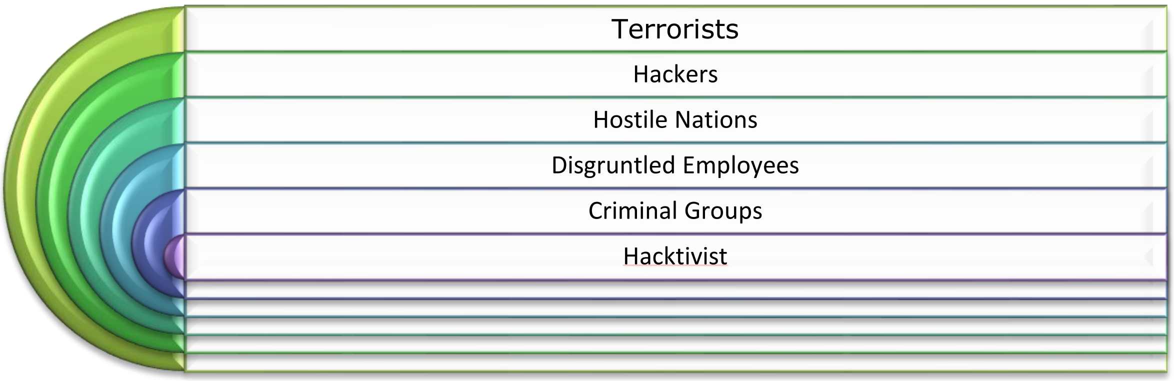
*"Cyber-attacks by hostile organizations, nations and criminals are on the rise, along with increase in cases of threat to governments, businesses and individuals by attempting to extract technical, financial, and national security information."*

***Gulshan Rai, Director General, Govt. Of India, Department of IT***

### Cyber threats: The invisible, borderless enemy

Cyber threats present some unique challenges, when compared to its more conventional counterparts like a war or a terrorist attack. *One*, it is near impossible to detect the exact origin as attackers tend to use hijacked systems or networks as proxies to launch an attack, in other words, the enemy is invisible. *Two*, in the matter of a few hours, it can spread across countries, causing widespread damage and potentially crippling critical digital infrastructure. So, the impact is not localized. *Three*, cyber attacks do not require access to expensive arms or military technology. Even a high school dropout with self-taught unethical hacking skills sitting with a run-down smartphone or tablet in a café can wreak large-scale havoc.

**Exhibit 1: The Cyber Attackers**



A case in point:

In July 2012, over 10,000 high-security Government of India email accounts were hacked. Among those targeted includedthe Prime Minister's Office, national intelligence agencies, and the ministries of Defence, Home Affairs, Finance and External Affairs. The scope and scale of the hackers' penetration took the government agencies by surprise, who were completely unprepared for an attack of this magnitude, even though there were prior warnings from the National Critical Information Infrastructure Protection Centre (NCIIPC).

And, lest one starts wondering if this was a one-off event or a recent phenomenon, that is not the case. The India Computer Emergency Response Team (CERT-In) estimates that there were 8,266 instances of cyber security breaches in 2009 alone, and this had shot up to 13,201 in 2011 and 22,016 in 2012[2].

There is no denying the fact that the number of breaches is going up and our cyber vulnerabilities are being exposed to the hacker community at large.

> ***"The number of mobile phones in the world is expected to rise to 8 billion by 2016 and broadband subscriptions to 3.5 billion by 2015, so arises the need to ensure cyber security in the country thus".***Gulshan Rai, Director General, Indian Computer Emergency Response Team

## A national security priority

Cyber security has emerged asa critical matter of national security. Our inability to act can put at jeopardy the national lifelines- telecommunication, power, public health, banking, aviation, and even people's lifetime savings like pension funds. Further, with the government's increased focus on e-governance and moving public services delivery like passport, driving license, birth certificates etc. online, the cyber infrastructure is emerging to be as crucial as, if not more than, physical infrastructure. And, protecting the cyber infrastructure therefore, has become as much of a national priority.

[2] *CERT-In report, Zee News*

Even though it may sound like a 'Prophet-of-Doom' statement, the destruction wrecked by this looming cyber war can easily dwarf anything that conventional warfare can achieve.

**Caselet 1: Attacking where it hurts the most**

In early July 2012, a staffer at the secretive National Technical Research Organisation (NTRO) noticed odd 'signals' on his monitoring system. Using complex algorithms that NTRO had been developing since 2010, he categorised these signals as a precursor to a major cyber-attack. The agency, run under the Prime Minister's Office, immediately sent a warning to all stakeholders, but it went unheeded.

On July 12, several high-level officials reported their emails had been hacked into - officials from the Ministry of External Affairs, Ministry of Home Affairs, Defence Research and Development Organisation (DRDO), and the Indo-Tibetan Border Police (ITBP) were part of that group.

The hackers even breached the main National Informatics Centre email server, which serves all government departments. An investigation put the total number of hacked accounts at roughly 12,000.

The hackers stole secret information such as deployment locations of troops and communication between ITBP (commanders) and Home Ministry officials.

## Why businesses and corporation must be worried

The Internet has become the preferred medium of communication, internally and with the external world, for all businesses. Not only that, increasingly critical data and business-sensitive information is being shared online, and also stored in a virtual environment on the cloud. In this virtual environment, a targeted cyber attack can be aimed at causing communication shutdown, stealing confidential data andintellectual property, and even sabotaging the company-wide intranet.

This threat scenario is not limited to large corporations only. Even though smaller businesses may not see themselves as a potential target for cyber-attacks, they may actually be even more vulnerable to cyber-hacking. As smaller businesses tend to cut costs by using third-party shared infrastructure and have leaner budgets to spend on cyber security measures, their 'wall of defense' in case of a cyber attack is weaker.

**Caselet 2: Putting virus into the drug**

In 2007, the IT team of a Chennai-based drug maker detected heavy traffic on servers connected to its research lab. The company was developing an anti-asthma molecule, and it suspected that a hacker was stealing research data.

Unable to trace the hacker, the company approached Mahindra Special Services Group (MSSG), a cyber security consulting firm, part of the Mahindra & Mahindra group. MSSG experts placed a dummy file containing a virus on the company's R&D folder that appeared to contain research data.

When the hacker returned, he went straight for the dummy file and the company traced him using the virus.

Here are some examples illustrating the nature of cyber threats to businesses, with motivations ranging from monetary gain to personal vendetta.

***Pune Citibank Mphasis Call Centre Fraud:*** Some call centre employees gained the confidence of customers, obtained their pin numbers and transferred money from their accounts online to bogus accounts.

***The Bank NJP Case:*** A man's former girlfriend, out of personal vengeance, sent emails to the man's foreign clients from fraudulent email ids using the bank's computers. The bank lost a large number of clients and this incident took the bank to the court.

***SMC Pneumatics (India) Pvt.Limited:*** This is actually the first case of cyber defamation of an employee. Someone named JogeshKwatra started sending derogatory, defamatory, vulgar and filthy emails to his employers to defame the company managing director.

***Andhra Pradesh Tax Case:*** The accused was running five businesses under the veil of one company and used fake and computerised vouchers to show sales records and evade tax.

# The Journey So Far

## A case of too little, too late

As a country, our cyber security evolution remains at a nascent stage, despite threats growing exponentially in the last decade. Even the most basic and critical layer of cyber security initiatives to protect our digital infrastructure- both in the public and private sector- has not been undertaken adequately so far.

Till as recent as July 2013, when the National Cyber Security Policy came into existence, we did not even have a cohesive critical ICT infrastructure protection policy.

In what can only be considered a strange irony, a country which is among the IT powerhouses globally, has lagged behind in its preparedness for even basic cyber security scenarios like cyber warfare, cyber terrorism and cyber espionage.

> ***"I think India is late in the game by about ten years. But at the same time I think the heart of the government is in the right place. It's a step in the right direction. The journey from a visionary cyber security policy to a tactical implementation to an actual change on ground is a long one."***Sanjay Bavisi, President and Co-Founder, International Council of E-CommerceConsultants

## Cyber Security Policy 2013

Following rising instances of cyber-attack episodes, lately, the Indian government has become more serious about securing the country's cyber space and formulated the National Cyber Security Policy (NSCP) of India in July 2013.

The following are the key measures mooted in the policy:

- Setting up a 24×7 National Critical Information Infrastructure Protection Centre (NCIIPC) for protecting critical infrastructure of the country

- One of the key agendas of the National Cyber Security Policy of India is to create a taskforce of half a million cyber security professionals in the next five years
- All organizations to designate a CISO and allot a cyber security budget
- Developing a dynamic legal framework to address cyber security challenges
- Encouraging wider use of Public Key Infrastructure (PKI) for government services
- Engaging information security professionals / organizations to assist in e-Governance initiatives, establish Centers of Excellence, cyber security concept labs for awareness and skill development on the PPP model - a common theme across all initiatives mentioned in this policy

Though the policy covers the broader issues pertaining to cyber security in the country, the question remains whether our country has adequately skilled workforce, and in adequate numbers, to drive cyber security measures?

More importantly, is the newly-formulated Cyber Security Policy holistic enough or is it missing the woods for the trees?

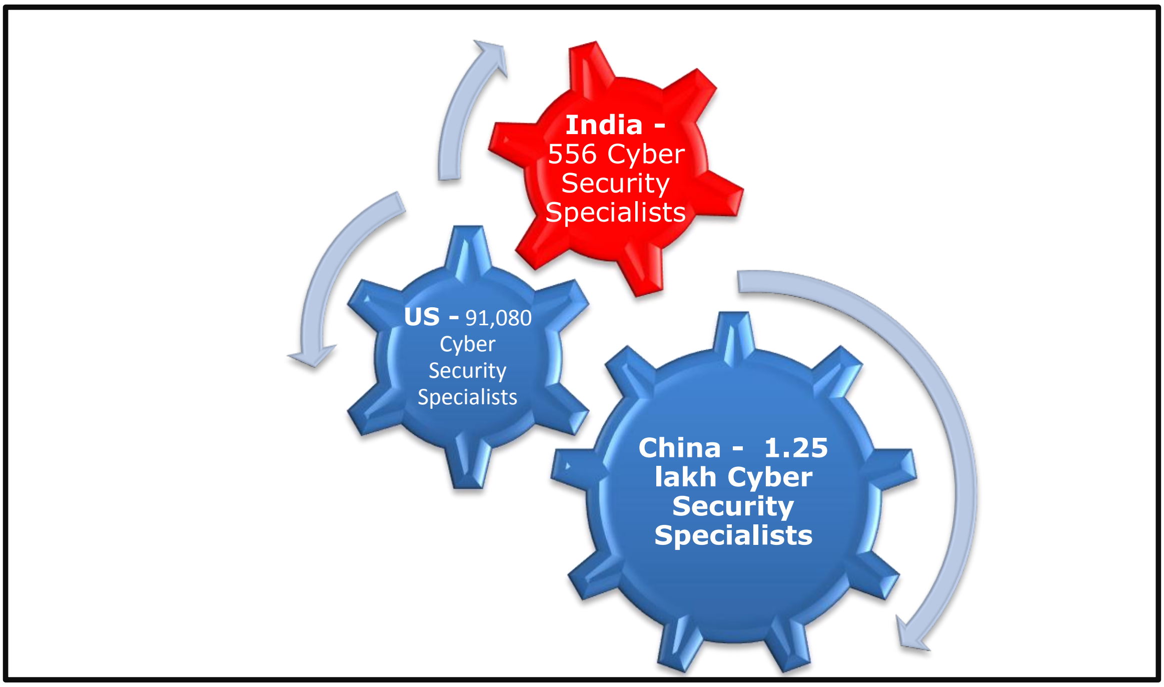
## Cyber Security- assessing the skill gaps

### An anomaly of numbers

Globally, India ranks third in terms of the number of Internet users, after the US and China, and by mid-2014 is projected to become the second largest. Further, the Internet user base in India is projected to grow six-fold between 2012 and 2017, at a compounded annual growth rate of 44%, according to a recent ASSOCHAM-KPMG study. The study also stated that India is amongst the top 10 spam-sending countries in the world alongside the US.

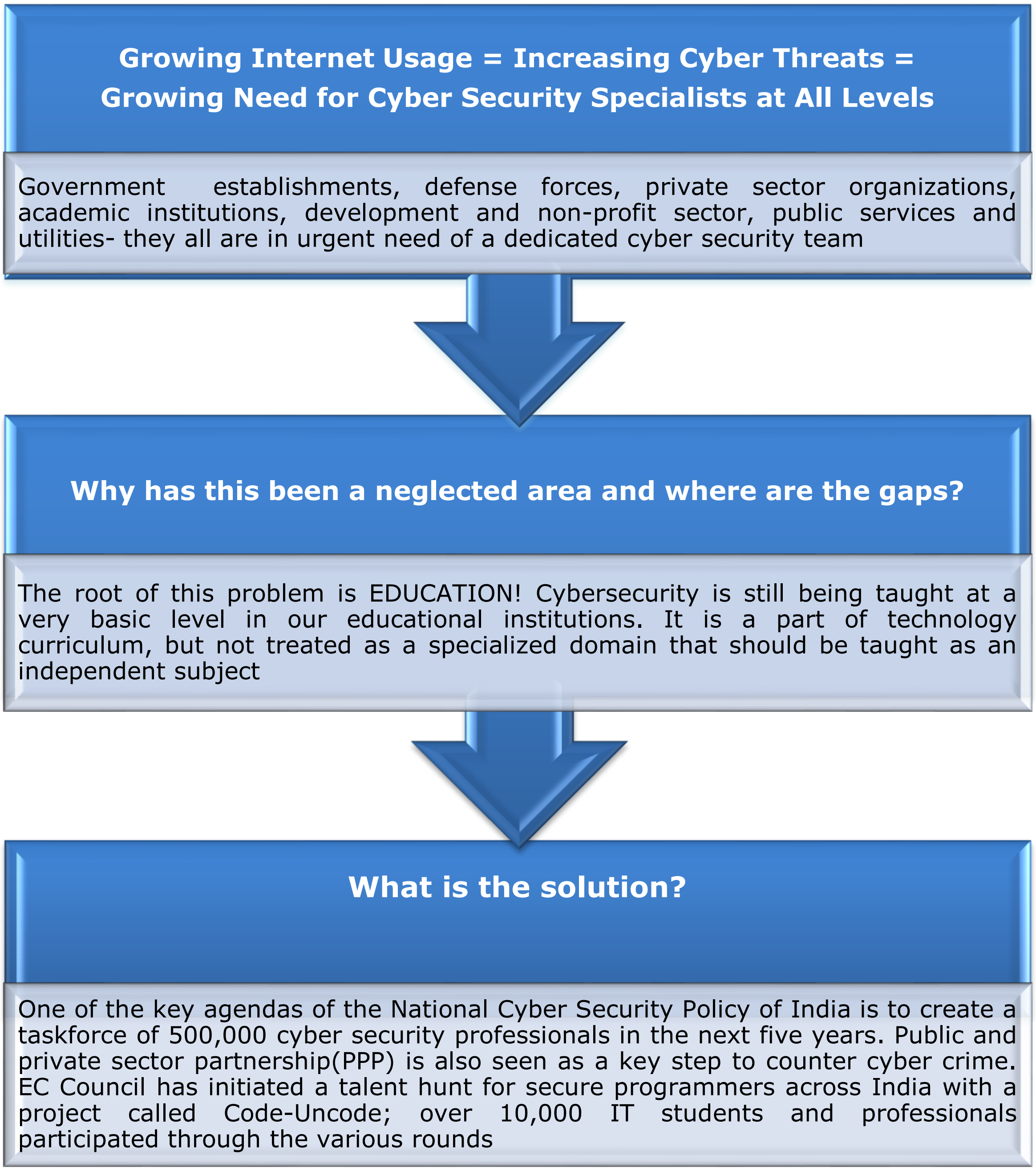
In such a scenario, one can assume that there would be a sizeable base of home-grown experts with cyber security skills in the country, at least in the private sector, which has scripted India's rise in the IT sector globally. But, the reality is alarming and comes as an eye opener. India has a negligible base of cyber security specialists, when compared to the US and China (*refer to Exhibit 2*) and when seen in the perspective of its Internet user base, the anomaly hits hard.

**Exhibit 2: Number of Cyber Security Specialists**


India - 556 Cyber Security Specialists
US - 91,080 Cyber Security Specialists
China - 1.25 lakh Cyber Security Specialists

Cybercrime has been affecting individuals as well as organizations in the country and the world over. There have been several instances of systems getting hacked in both private and public sectors, which calls for an urgent need to contain this crime and secure the country from it.

**Exhibit 3: Creating Cyber Specialists**



**Growing Internet Usage = Increasing Cyber Threats = Growing Need for Cyber Security Specialists at All Levels**

Government establishments, defense forces, private sector organizations, academic institutions, development and non-profit sector, public services and utilities- they all are in urgent need of a dedicated cyber security team

**Why has this been a neglected area and where are the gaps?**

The root of this problem is EDUCATION! Cybersecurity is still being taught at a very basic level in our educational institutions. It is a part of technology curriculum, but not treated as a specialized domain that should be taught as an independent subject

**What is the solution?**

One of the key agendas of the National Cyber Security Policy of India is to create a taskforce of 500,000 cyber security professionals in the next five years. Public and private sector partnership(PPP) is also seen as a key step to counter cyber crime. EC Council has initiated a talent hunt for secure programmers across India with a project called Code-Uncode; over 10,000 IT students and professionals participated through the various rounds

## What experts say about skill gaps

According to **Vineet Kumar, the Chief Technology Officer of Jharkhand Police**, *the problem of skillset matching arises because there is a significant difference between what knowledge is being required for practical problem solving and what is being actually imparted in the universities currently. No specialised courses are currently available which will address specifics, such as TADA Security. The courses on offer are very basic in nature with no advanced curriculum being designed to address real life needs.*

Similar thought is reflected in the opinion of **Akash Agarwal, Country Manager of EC Council**. According to him, *cyber security is still being taught at a very basic level in our educational institutions. It is part of the curriculum but not being treated as a specialized domain that should be taught as an independent subject. There is a need for stronger collaboration between industry and academia to address this at the earliest.*

*India is still in the nascent stages of forming a cyber securityecosystem and promote sharing of information within the ecosystem and between companies.*

*"In Canada, we use the mantra of 'when people are being chased by a bear, you don't need to be faster than the bear, you just need to run faster than the guy running next to you'. This analogy does not work in cyber security because not only will the bear get the laggard, but will very quickly turn on the rest", opines* **Adel Melek, Managing Director for Global Enterprise Risk Services, Deloitte.**

# The Case of Israel- A 'Cyber Secure' Country

## Cyber-attacks: The evolution of modern warfare

*"Everybody understands that you buy Swiss watches from Switzerland and information security from Israel."*

***UdiMokady, CEO, CyberArk Software, Israel's largest private cyber security company.***

How did Israel, a nation with a population of just around eight million and an area so small that it is half the size of the Mediterranean exclusive economic zone, emerge as the **Go-To destination for cyber security** globally?

Before we try and understand the 'How', it would be worthwhile to delve into the 'Why'. The dictum, 'Necessity is the mother of invention', won't be far from truth in this case. Created in 1948 as an independent Jewish state in the aftermath of World War II, a devastating chapter in human history, Israel is in an unenviable place geographically. Flanked on one side by the Mediterranean Sea and landlocked on all other sides by its Arab League neighbours who have been historically opposed to its existence as a nation state, Israel lives in a constant shadow of violence and sovereign threat. Further, the Jewish nation's small size and population, a relative scarcity of natural resources, and a largely arid landscape- all of these are factors that place significant limitations on how it can respond to the ever-present threats.

But, instead of being overwhelmed by these limitations, Israel has displayed extreme ingenuity, turning them into opportunities and spawning innovation.

In the initial decades that followed the creation of Israel, the threats facing the country were predictable and conventional in origin, and could, therefore be countered by building military might and warfare capabilities. However, in the later years with the emergence of militant groups like Hamas and their resorting to indiscriminate rocket strikes, the threat to civilian life has become more dispersed, more frequent and difficult to contain. Israel Defense Forces (IDF) estimates that, since 2001, almost 13,000 rocket strikes at an average of three per day[3], have been launched on Israel's civilian population by Hamas and similar groups. Looking for a solution, Israel turned to advanced technology to counter the threat of missile and rocket attacks from renegade terrorist groups or in case of a conventional war with one of its Arab neighbours. The country has developed short-range and long-range missile defense systems and radar technology, e.g. the renowned Iron Dome, which are amongst the most advanced globally.

In this cat-and-mouse game, its adversaries have not been sitting idle, but keeping Israel on its toes. Taking the level of threat to an entirely different and potentially limitless arena in today's Information age, countries and militant groups opposed to Israel, have taken with vengeance to the latest arsenal on the block, **Cyber Warfare**.

Manifesting in its most visible and virulent form as **Hacking**, Israel's civilian and military networks are being increasingly targeted by hacker groups, and even inimical governments. Let us consider some alarming examples[4].

- On the twelfth 9/11 anniversary this year, three hacker groups- Anonymous, AnonGhost and Fallaga- plotted to attack Israeli websites in an operation dubbed #OpIsrael #Reborn, inviting others through a YouTube video to participate.
- In Apr, 2013, Israel's most critical networks were targeted in a coordinated cyber-attack by multiple hacker groups (not for the first time) who threatened to "wipe Israel off the Internet", but the country's cyber security teams were successful in negating the threat, once again.

[3] Israel Defense Forces, IDF
[4] The Jerusalem Post

- In Jan 2012, details of tens of thousands of Israeli credit cards were stolen by Arab hackers and published online.
- In Jan, 2012, the Israel Fire and Rescue Services website was hacked by a group referring to itself as the Gaza Hacker Team. The hackers wrote "Death to Israel" in Hebrew on the website and superimposed on it a defaced photo of Israel's deputy foreign minister, Danny Ayalon.
- In May 2011, critical state infrastructure like the water system and electrical grid, was targeted unsuccessfully by cyber-attackers, which came to light when Shin Bet, Israel Security Agency detected 'fingerprint' and 'tracks' of attempted attacks.

How has Israel, time and again, foiled these persistent and large-scale cyber-attacks, with much aplomb and precision?

## Israel's march to cyber security

Like they say, 'Rome was not built in a day', and taking a leaf from this adage, we can understand how Israel has gone about developing its cyber security expertise to a level unparalleled globally. Looking at this achievement from a skill development perspective, there are three key approaches that emerge as the fulcrum of Israel's strategy.

### Developing a 'Cyber Army'

The Israel Defense Force (IDF) has created **two elite units for cyber warfare-** C4I and Military Intelligence- the former stands for Command, Control, Communications, Computers and Intelligence. Rolling out a multi-year plan to be at the cutting edge of cyber warfare, these two units have been recruiting talented computer experts, many of whom are young enough to yet earn their college or even high-school degrees.

Further, the IDF has structured the two units to create focused expertise- Military Intelligence's Unit 8200 is tasked with building offensive capabilities, while a dedicated division has been created within C4I for defensive operations. It is suspected that Unit 8200 was behind a virus attack, referred to as Stuxnet worm, on Iran's first nuclear installation in Sep 2010 that infected worker's computers and stopped work temporarily at the power plant.

## Defense-Civilian partnership for a cyber community

The Israel government has actively sought out private sector institutions and the civil society to create a wide network of cyber security experts. In 1997, Tehila, an e-government institution was created to meet the cyber threat, followed by National Information Security Authority in 2002, which is responsible for preventing cyber-attacks against critical infrastructure[5]. Since January 2012, the Israel National Cyber Bureau (INCB) has been in operation, and has been instrumental in creating a **national cyber defense policy**, partnerships with the private sector, and linking domestic and international cyber defense players.

Example of some unique initiatives by INCB includes the establishment of a national cyber situation room.This is tasked with forming the cyber defense matrix and facilitate information sharing between the defense community, the public sector and the private sector. Further, between 2013-15, the Ministry of Economy plans to invest USD 22 million in R&D for the cyber defense industry.

Extending the partnership to academic institutions, the government plans to create a **'cyber defense hub'** by moving all governmental and military institutions which address the cyber threat to the city of Beer Sheva. Here, they will all be linked to the world-class academic infrastructure of Ben-Gurion University and a newly constructed industrial park serving a flourishing hi-tech industry.

[5] Israel Ministry of Foreign Affairs

## Promoting cyber entrepreneurs

Culturally and socially, Israel has been a hotbed of entrepreneurial activity, with several inspiring stories of soldier-turned-entrepreneur-turned-serial investor. This has created an ecosystem where start-ups are nurtured and supported actively, and the cyber security space is no exception to this phenomenon.

There is no dearth of **cybersecurity start-ups** in the country, founded by young and gutsy entrepreneurs with significant military stints under their belt, which gives them a hands-on understanding of the nature of cyber-threats, enabling them to pioneer relevant solutions. Companies like Lacoon Security, Zimperium and Cyvera are operating at the cutting edge of innovation, developing new solutions in cyber security for businesses, governments and individual computer owners.

Cyvera, for example, takes a novel approach to cyber-attacks by proactively closing off the path of attack, instead of reacting to cyber-attack events and coming up with a patch, the way that most anti-virus programs work. Choking off the paths used by hacktivists is the easiest and the most efficient way to prevent attacks altogether[6]. Lacoon Security is another company taking a preemptive approach. The start-up, which recently raised USD 2.5 million in a funding round, focuses on mobile security, aiming to counter data theft from smartphones and tablets. Lacoon produces systems that protect both user devices and networks against mobile malware by using a cloud solution. Zimperium, in a radical move has hired the celebrated hacker, Kevin Mitnick, a master hacker-turned-good guy on its advisory board. Kevin served five years in prison for cyber-crimes committed during the 1980s and 1990s. The company integrates artificial intelligence with behavioral analysis to generate an automatic optimized set of rules based on system experience, identifying rogue data and keeping it off Android devices before it has a chance to "settle in" and create havoc.

[6] Times of Israel

## Developing an Action Agenda for Skill-building

Considering the significant and increasing threats to our national, financial and personal security, there is an acute need for building cyber security skills at multiple levels. Moreover, the yawning gap between what is required and where we are can only be bridged by taking concerted action on a war-footing.

What should be the key elements of our action agenda to develop cyber security skills?

To understand the various dimensions of this endeavour, we have researched a diverse range of material, talked to experts and practitioners, looked into Israel's example and distilled key learnings.

### Support Cyber Warriors- Ethical Hackers

Cyber security requires unconventional approaches and goes much beyond antivirus and firewall solutions. The best way to be safe on the Internet is to understand how hackers operate in the cyber world and then develop ways and means to combat them. Hence, there is a need to train our ethical hackers into tomorrow's Cyber Warriors, by identifying their talent early, and then imparting them appropriate training and skills.

> ***"Unless and until education system changes, there is no point in producing 500,000 professionals, the goal that Cyber Security Policy has set. Train the trainer should be the motto and not producing professionals based on the current curriculum which lacks practical aspects"-***
>
> ***Saket Modi, Ethical Hacker and CEO, Lucideus Tech.***

India has no dearth of ethical hacking talent, the most prominent name being Ankit Fadia, who by the age of fourteen had achieved worldwide fame as an ethical hacker, and is today a sought-after expert in the area. This year, for the first time, a team of six ethical hackers from Hyderabad has qualified into the

Global CyberLympics Hacking Championship being held at Atlanta, a prestigious ethical hacking, computer forensics and computer network defence competition[7].

There is a need to develop curriculum on ethical hacking and integrate it with regular courses in computer/engineering/electronics space. The courses in cyber security also need to be identified at various levels from Beginner to Advanced, with appropriate recognition and certification by universities.

## Developing Cyber Security Centre of Excellence

There is need to nurture a Centre of Excellence in Cyber Security to bring synergy between latest advancements, research and training. The Centre would be responsible to bring cyber training to school/college/Professional level and also work as a depository of all available expertise in India at several places, so that when needed, the most appropriate expert is assigned to particular cyber attacks.

## Developing cyber defense hubs in each region

Currently, what we lack in India is an interface, a thriving ecosystem of cyber security expertise, research and innovation. Bringing academia and research, private sector, government cyber intelligence agencies, entrepreneurs and funding agencies on one platform, the way Israel has accomplished at the city of Beer Sheva, where Ben-Gurion University is located, will lead to innovative solutions and advanced skill development in the field.

However, considering our vast geographical and population spread, we will have to create **multiple cyber defense hubs**. A good start can be do align these hubs with the Indian Institutes of Technology (IIT) campuses in North, West, East and South.

[7] Times of India

## Introducing cyber security super specialization

India is renowned the world over for its top-tier technology institutes, which have regularly contributed innovators, entrepreneurs and business managers over the years. A focus on building such a talent pool in the domain of cyber security is the need of the hour.

A good start would be to introduce various short-term, long-term, certification and advanced learning programs at the graduation and post-graduation level in cyber security as a super specialization.

## Training netizens in cyber security skills

Although, India has tens of millions of Internet users, the level of awareness is very low when it comes to protecting/sharing confidential information online, conducting safe e-commerce transactions, and maintaining passwords, email accounts etc.

A large majority of Internet users, including even those with post-graduate qualification, are not aware of basic security guidelines to follow, when online. Consequently, each individual PC, laptop or smartphone is a gateway through which a cyber-attack can be launched, e.g. a virus, eventually spreading through and sabotaging a wide network.

Therefore, it becomes essential to create a **cyber security literacy framework** through ongoing campaigns, with active participation of all key stakeholders e.g. social media sites, banking and financial service providers, and e-commerce businesses.

CMAI Association of India
Communication Multimedia
And Infrastructure

NK Goyal
President CMAI
+91 98111 29879
President_cmai@cmai.asia
www.cmai.asia
www.cmaievents.com

## About CMAI

CMAI Association of India is apex premier and foremost non-profit trade promotion organization based in India with MOU partners and representatives spread across globe. CMAI is prominent trade association promoting growth in communications, manufacturing trade sector through Legislative and Regulatory Advocacy, Research, Exhibitions, Trade shows, Conferences and Seminars, Technology events, Buyer sellers meets, B2B meetings, promotion and fostering : business and strategic relationships. CMAI is the only trade organization bringing in focuses harmony in between manufacturing across all sectors including ICT, Communications, Multimedia and Environmental Management policies. CMAI assists in promotion of technology innovations, manufacturing and communications sector and for policies concerning environmental, pollution and health. CMAI, as a professional registered association, has become extremely pro-active, forward looking and effective catalyst between the Government, industry and the consumers at large. CMAI has been successful in influencing the Government in shaping India's economic, trade, fiscal and social policies which will be of benefit to the country as a whole and the trade and industry in particular. CMAI caters services to various constituents comprising multinational companies, top corporate, medium and small scale units representing and striving hard to create a conducive environment for the businesses to compete globally. It assists manufacturers to maximize competitiveness on the domestic and international markets.

## CMAI Core Mission

- To assist trade, businesses and manufacturers in development of domestic and international markets.
- To collaborate with Government and industry to promote business, trade, manufacturing, communications.
- To provide consultations, advice guidance and information for business alliances, trade promotion.
- To develop an effective platform for attracting major buyers and sellers face to face in various trade shows and delegations, conferences and forming partnerships with various overseas organizations and enhancing a synergistic effect through convergence and related industries giving opportunities and access to members to the newest technologies and industry information.

## CMAI is involved

- In developing scientific knowledge and practical means for protecting man and his environment from the harmful effects of environmental hazards like e waste, radiations etc.

- To further the exchange of scientific and technical information relating to the science and practice of environment protection.
- In encouraging research and scientific publications dedicated to the science and practice of in this field.
- In promoting educational opportunities in those disciplines which support the science and practice of environment protection.
- Assisting in the development of professional standards for environment protection.
- In supporting the activities of other societies, associations or organizations, both national and international, having any activities or objectives relevant to above In brining awareness of environment hazards from e waste, pollution, plastics, asbestos etc. amongst the users and public in general.
- In encouraging adoption of appropriate means for avoiding or reducing environmental hazards and exposure in the applications of radiations and nuclear technology, such as power generation, industry, medicine, agriculture, scientific research etc., thereby maximizing the benefits which are derived out of these applications while minimizing the risks.
- In facilitating contacts and exchange of information amongst specialists in environment protection and related disciplines in e waste, pollution, green policies within India and in other countries.

## CMAI support to Industry and Trade

CMAI derives its strength from its data base. CMAI provides with public policy establishment, industry competitiveness upgrade, development strategy and planning, marketing strategy and research, HR management, IT programming and management. The CMAI Members ranges from industrial users in electronics, telecommunications, energy, finance, automobile, telecom, ICT to autonomous Institutes like Research bodies, trade associations, policy forums to Government departments at all levels and diversified industrial parks.

- CMAI champions the developmental and promotional issues on behalf of the industry, trade relating to Manufacturing, Communications, and ICT, Environmental industry.
- CMAI seeks to provide a common platform for all members of the industry to interact, work together.
- CMAI seeks to keep its members abreast with upcoming technologies and industry updates by information dissemination and by organizing regular seminars and info sharing sessions
- CMAI works to provide helpful information to members to enable them to face ongoing challenges in business development, technology or economic situations prevalent in world.
- CMAI publishes Daily News Letter in association with its partner Telecomwatch, Telelinkers, which is distributed complimentary to all the members and other stake holders.
- CMAI reinforces its presence in the industry by participating in international/regional conferences and exhibitions, facilitating networking sessions with overseas business, industry and trading partners, representing the industry in National and International standard and other committees, forums and establishing regular dialogues between the industry and Government.

## ***CMAI Flagship Events***

**CMAI NTA ICT World Communication Awards & National Education Awards**

May I Siri Fort Auditorium I New Delhi I India.

**CMAI India International Communications and Electronics Fair**

Mobiles Tablets Consumer Electronics

December I Pragati MadianI New Delhi I India

## ***Other CMAI Events***

- CMAI Sai Sandhya, New Delhi, January Every year
- CMAI CES Delegation, Las Vegas, January Every year
- CMAI Delegation to Mobile World Congress, Barcelona Feb, Every Year
- CMAI Delegation to World Electronic Forum, May Every year
- CMAI Delegation to Asia Electronic Forum (AEF), Every year
- CMAI Delegation to Asian Telecom Information Exchange
  - Forum(ATIE), Every year
- CMAI Delegation to Commasia, Singapore, June Every year
- CMAI CES Sinoces, Qingdao Delegation, July Every year
- CMAI Delegation to China Mobile Phone Industry Exhibition
  - Shanghai, July, Every year
- CMAI Delegation to Kunshan Electronics Show, Kunshan July-August, Every year
- CMAI Delegation to Korea Electronics Show Korea, October Every year
- CMAI Delegation to Taipei Int'l Electronics, Taiwan, October Every year
- China Shenzhen Mobile Phone Industry Exhibition,
  - Shenzhen, China November Every year
- India Telecom , New Delhi, December Every year

CMAI organizes several events in educational sector with AICTE and more than 200 universities and 25,000 colleges across the globe.

**About Dion Global Solutions**

Dion Global Solutions Ltd. is a rapidly growing Indian MNC with more than 25 years of experience in the global financial sector, as a provider of technology, consulting, website, information and research solutions. The company's client base includes leading brokerages and financial institutions in India and overseas. Dion has been expanding its global footprints organically as well as through acquisitions, strategic stakes, and joint ventures.

In website design and development, data, financial content, business and financial research, information and search engine-social media optimization services, equipped with a proprietary research platform, an experienced leadership and delivery team, and state-of-the-art infrastructure, Dion provides insight-driven and cost-effective solutions to financial institutions, brokerages, and multinational corporations.

Dion's expertise in the area of financial data and content is being acknowledged as best-in-class. Dion has been empanelled after qualifying through a rigorous evaluation process by the SEBI-promoted National Institute of Securities Markets (NISM) as its Content Partner in financial literacy and intermediary certification initiatives.

Key facts on Dion include:

- Part of a large diversified transnational business group, Dion caters to the software, information, and content needs of financial institutions and Fortune 1000 companies
- More than 630 clients across 86 countries, including leading brokerages and financial institutions in India whose financial portals have been developed and are being managed by Dion
- Providing solutions for: Trading, Clearing & Settlement, Governance, Risk & Compliance, Messaging, Customer Management, Technical Analysis, Derivatives Analytics and other Value Added functions
- In-depth Research & Information services capabilities
- Market presence in Asia Pacific, South East Asia, Europe, Middle East, USA & Latin America
- Team of over 600 highly skilled personnel across 18 countries
- State-of-the-art product development, content delivery and innovation centers across three locations in India-Bangalore, Mumbai and Delhi-NCR (Noida)
- Strategic stakes in Chase Cooper, London  and Marco Polo Networks, New York

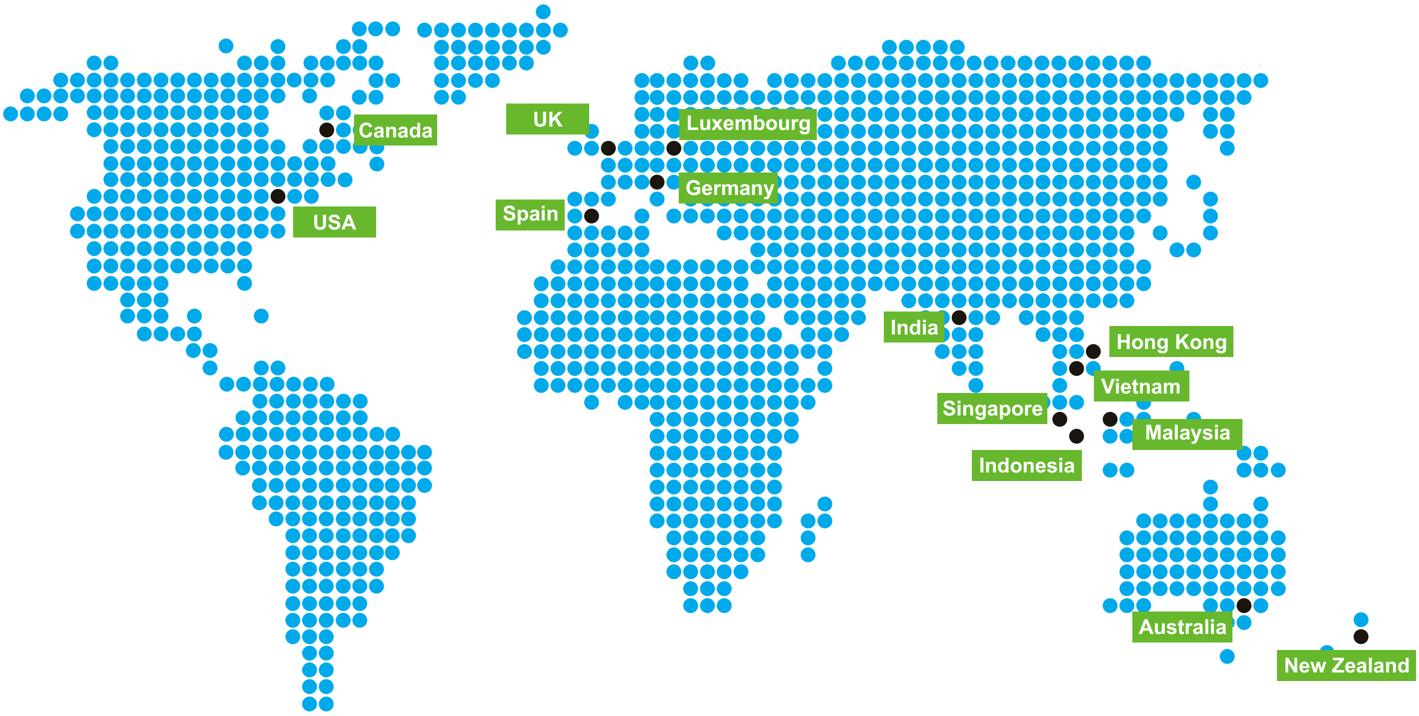
## About us

Dion is the trusted technology partner to the financial services industry. Dion's aim is to take the pain and risk out of financial technology in a constantly changing market, by providing a consistent, reliable and approachable source of value added solutions. From flexible pricing models, to fuss-free implementations, Dion's business model is about providing a straightforward approach that is responsive to client needs and enables them to turn financial technology into real business opportunities.

The company draws on its presence across the financial markets, the depth of its global expertise and the breadth of its product development resources to serve the specific and localised needs of its clients. Dion continually strives to make available new solutions that deliver the value that clients are looking for, both through in-house development and strategic acquisitions. As a result, Dion is the single source for a comprehensive and developing range of solutions, from which financial services firms can select those that meet their business needs both now and in the future.

The company has over 550 clients in more than 80 countries supported by a worldwide staff of 600, including 200 in product development. Company provides solutions that span investment, retail and commercial banking, institutional trading and investment and private client wealth management and stock-broking.

## Our global footprint


Canada
UK
Luxembourg
USA
Spain
Germany
India
Hong Kong
Vietnam
Singapore
Malaysia
Indonesia
Australia
New Zealand