Rijksdienst voor Ondernemend Nederland

Cyber Security in India

Opportunities for Dutch companies

>> Duurzaam, Agrarisch, Innovatief en Internationaal ondernemen

Index

Executive Summary

The Cyber Security Market in Asia Pacific, which stood at USD 17 Bln in 2015, is poised to grow at a CAGR of 12.3%, reaching USD 54 Bln by the year 2025. According to industry estimates, the increasing incidents of cyber-attacks and data protection efforts globally, would create USD 35 Bln revenue opportunity and would provide employment for about a million professionals in India by 2025. However, to capitalize on these opportunities, the Indian Cyber Security industry has to overcome the challenges it faces, and has to come up with a clear and organized agenda, which would involve, *inter alia*, strong Cyber Security policy and regulation, focus on capacity building both at government and industry levels, developing new products through R&D collaborations, supply of new products and services and cyber forensics. The Netherlands, with its long heritage and strong expertise in the sector, is well positioned to capitalize on these opportunities and support India in achieving its ambitious goals in the field of Cyber Security. This report would elaborate on what are the challenges faced by the Indian Cyber Security industry and provide insights into how the Dutch Cyber Security industry could assist the industry in India in overcoming those challenges.

Introduction

The threat from professional criminals and state sponsored saboteurs in cyber space is growing and continues to become more sophisticated. State sponsored saboteurs focus on economic and political espionage and on making preparations for digital sabotage. Not only are the number of countries that are developing digital attack capabilities increasing, the attacks that are carried out are also becoming increasingly complex. Combined with it, is the numerous attacks that the digital infrastructure of countries face on a daily basis from non-state actors. This forms a direct threat to the economic interests and national security of countries. These developments call for an increased effort to strengthen the cyber-security infrastructure of countries and thereby better protect their vital interests.

Cyber attackers are highly motivated, well-funded and technically advanced. Their attacks pose a threat to national initiatives such as Smart Cities, E-Governance and digital public identity management. Government and military organisations and other businesses store and process significant volumes confidential data, regularly transmitted across networks, thereby increasing their exposure to cyber threats. The potential damages can't only lead to monetary losses, but also put national security at risk if critical information infrastructure is targeted.

India is seen as a preferred outsourcing destination globally and key global brands such as Apple, Sapient, Citi Bank, HSBC, Bank of America, DSM etc., have set their global delivery centres, shared services & support services in India. India is currently rolling out the world's largest ICT programme called 'Digital India', which is focused on efficient service delivery, governance, improving access from education to health, as well as moving India towards digital currency, to open up India to the digital age. The Indian digital landscape has seen an unbelievable amount of transformation in a short duration of time, having grown substantially over a relatively shorter period. This obviously creates vulnerabilities that state and non-state actors could potentially exploit for their selfish gains.

The programmes that are being undertaken in India in the cyberspace, both on Government level and private level, are enormous and provide a lot of opportunities for Dutch businesses in this crucial phase of the Indian digital transformation. This report shows how The Netherlands is best poised to capitalize on the economic and social opportunities of digitalisation in India a secure way and to protect national interests of India in the digital domain.

Evolution of global Cyber Security industry

The Cyber Security industry in India was not always as sophisticated as it is today. As the cyber landscape became increasingly complicated, so did the Cyber Security industry. The three main evolutionary phases in the history of Cyber Security are as follows:

I. **VIRUS Protection**: In the first stage, cyber secutity concepts were largely focused on protecting individual computers from Vital Information Resources Under Siege (VIRUS) attacks. This largely took the form of simple Anti-VIRUS softwares that could be purchased and installed in individual computer systems. VIRUS protection focussed on ensuring that IT systems and devices performed as expected, upon installation of the anti-VIRUS software.

II. **IT and Network Security**: In the next phase of evolution came the concept of IT and Network Security. This phase was the direct consequence of the realization that attacks to individual computers can affect the whole networks to which they are connected to. IT and Network Security focuses on the protection of the devices and the information assets passing through the network, by installing firewalls and network security software.

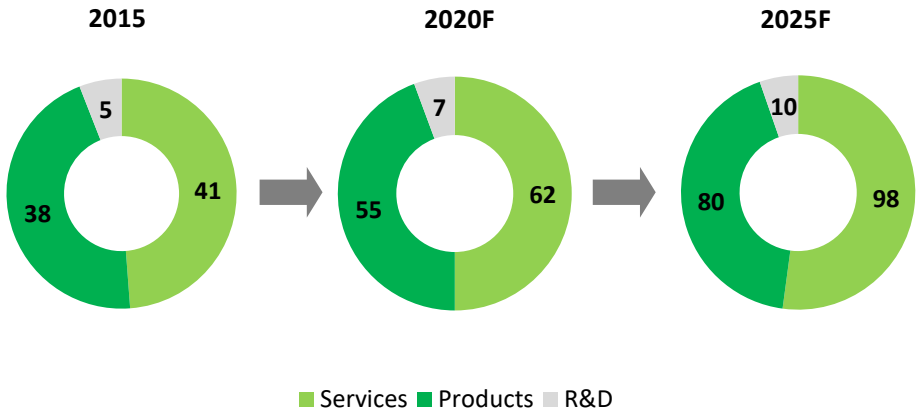
III. **Cyber Security**: In this phase, where we are currently, Cyber Security and information assistance has taken on a more comprehensive systems, data and mission assistance role. The threats have become far more complex, which necessitates far more complicated responses as well.

Cyber Security Market Trends

According to the Data Security Council of India (DSCI), the current size of the global Cyber Security industry is estimated to be USD 80 Bln and is projected to grow to USD 190 Bln by 2025. The market is expected to grow at a compounded annual growth rate (CAGR) of 8.2% from 2015-2025.

On the products side, the Cyber Security market has three dimensions – (a) supply of products, (b) supply of services and (c) R&D. While the demand side companies focus on industry verticals and geographies, the supply side companies focus on the supply of various Cyber Security products and services in the market.

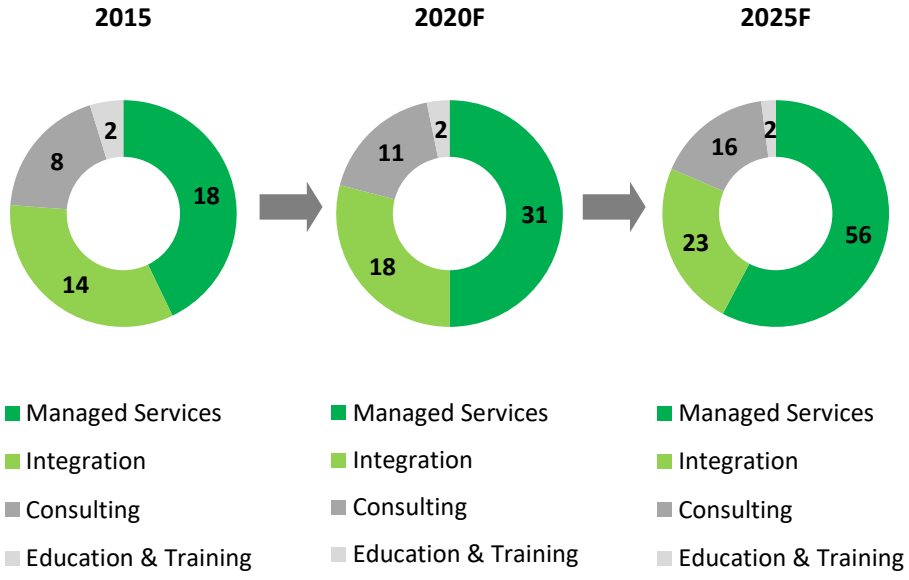
Global Cyber Security Market – Evolving Trends in Product Types (in USD Bln)



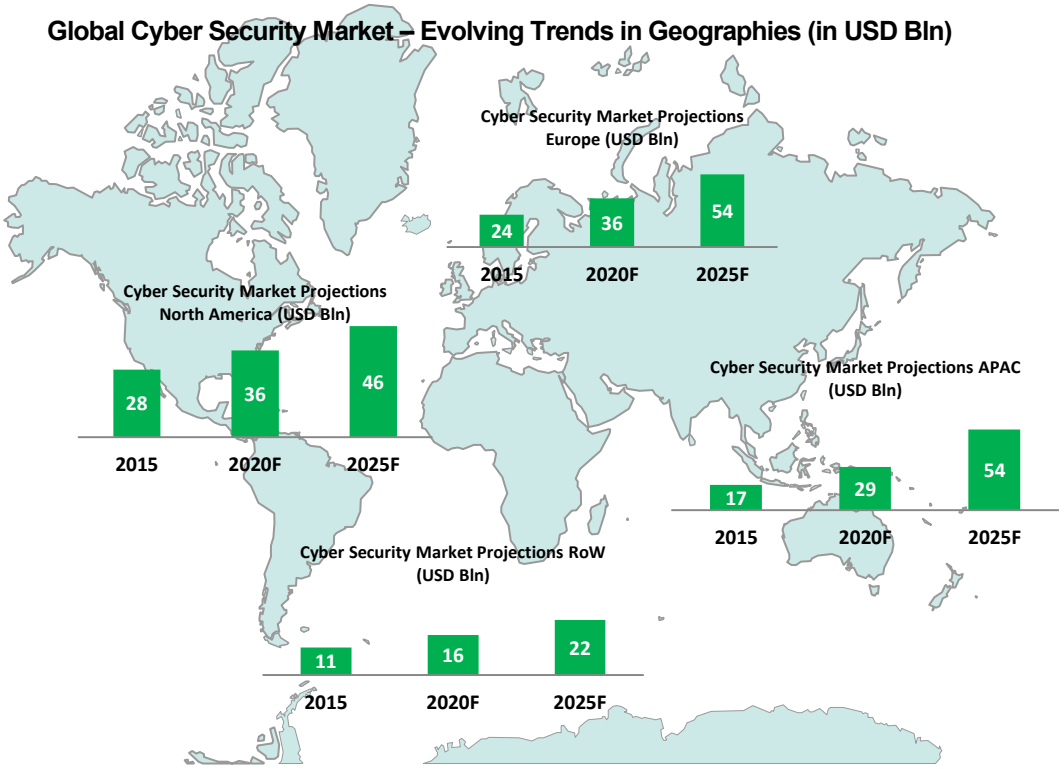
Source: Source: DSCI-Growing Cyber Security Industry-Roadmap for India, Dec, 2016

Coming to service types, the Global Cyber Security Market can be classified into following four sub-groups: (a) Managed Services, (b) Integration, (c) Consulting, and (d) Education & Training.

Global Cyber Security Market – Evolving Trends in Services Types (in USD Bln)



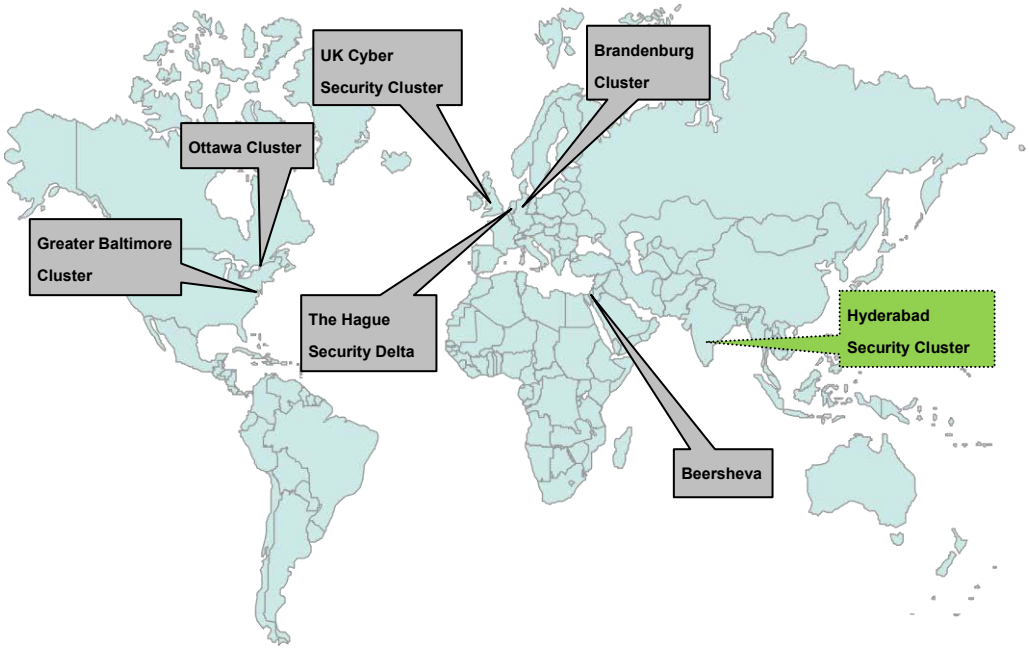
Source: Source: DSCI-Growing Cyber Security Industry-Roadmap for India, Dec, 2016



Source: Source: DSCI-Growing Cyber Security Industry-Roadmap for India, Dec, 2016

Global Cyber Security Clusters

Globally, there are quite some prolific Cyber Security clusters, performing cutting edge research in Cyber Security and changing the market landscape significantly with their prowess and innovation. A few such clusters are being outlined and compared below:



Note – This map is not to scale. Political demarcations may be inaccurately depicted.

	Ecosystem Variables			
	Policy & Financing	Domestic Market	Infrastructure	Talent
Greater Baltimore Cluster (USA)				
Hague Security Delta (The Netherlands)				
Beersheva (Israel)				
Berlin Brandenburg Cluster (Germany)				
Ottawa Security Cluster (Canada)				
UK Cyber Security Cluster				

Source: Source: DSCI-Growing Cyber Security Industry-Roadmap for India, Dec, 2016

	Differentiators			
	Cost Advantages	Product/Service Focus	Innovation Dominance	Focus Markets
Greater Baltimore Cluster (USA)		Services		
Hague Security Delta (The Netherlands)		Products		
Beersheva (Israel)		Products		
Berlin Brandenburg Cluster (Germany)		Products		
Ottawa Security Cluster (Canada)		Services		
UK Cyber Security Cluster		Services		

Source: Source: DSCI-Growing Cyber Security Industry-Roadmap for India, Dec, 2016

Opportunities in the Indian Cyber Security market

According to the National Association of Software and Services Companies (NASSCOM), India is one of the most vulnerable nations in the world when it comes to cyber-attacks. As per NASSCOM estimates, the increasing incidents of cyber-attacks and data protection efforts globally would create USD 35 Bln revenue opportunity and would provide employment for about a million professionals in India by 2025.

Growth in the market is expected to be driven by rising number of government initiatives towards digitizing government sector entities and processes, healthcare, banking and financial services industry, education and other vital sectors of the country. Government schemes such as 'Make in India', 'Start-Up India' and 'Digital India' supplements the growth of Cyber Security market in India and is a linking pin towards Public-Private Partnership (PPP) models.

India has seen a tremendous growth in tech savvy population, with mobile phones being the first digital medium. At the same time, there has been substantial growth in IT spending in India and scaling up in the use of technologies such as Internet of Things (IoT), Cloud Computing, Artificial Intelligence (AI) and Block Chain. It is expected that these will rise further, transforming India into one of the largest internet based markets across the world.

According to the web portal Research and Markets, the current size of the Cyber Security industry in India is estimated to be USD 3.8 Bln. Market watchers estimate that the Indian Cyber Security market would grow at a CAGR of 15 – 20% during the years 2018-2023.

What are the main Cyber Security challenges in India?

1. **Lack of national level architecture for Cyber Security** – In India, Critical infrastructure is owned by both Public Sector and Private sector, both operating with their own norms and protocols for protecting their infrastructure from cyber-attacks. The armed forces too, have their own firefighting agencies. However there is no national security architecture that unifies the efforts taking place in the public sphere and in the private sphere, to be able to assess the nature of any threat and tackle them effectively, in a coordinated fashion.

2. **Shortage of trained workforce** – Although India is rife with a young workforce with considerable IT prowess, there is a dearth of talent when it comes to specific niches, such as Cyber Security. The demand for talented and skilled labour

far outgrows supply, and with the market poised to grow further substantially, this gap is likely to widen further.

3. Lack of co-operation – Unlike countries or states, in cyberspace there are no boundaries, thus making the armed forces, critical national infrastructure, banking functions, etc. vulnerable to cyber-attacks from anywhere. This could result in security breaches at a national level or state level, causing loss of money, property or lives. To respond to possible threats on the country's most precious resources, there is a need for a technically equipped multi-agency organization that can base its decisions on policy inputs and a sound strategy.

4. Lack of awareness – There is no national regulatory policy in place in India for Cyber Security. There is also a worrying lack of awareness about cyber laws and regulations at both corporate levels as well as individual levels. Domestic internet users can protect and be protected from the cyber-attacks only if there is a guided and supervised legal framework.

5. Lack of uniformity in devices used for internet access – With varying income groups in India, not everyone can afford sophisticated phones. In India, less than 1% of mobile phone users have access to mobile phones with higher security norms. The widening gap between the security offered by the high-end mobile phones and lower cost mobile phones in the market make it almost impossible for legal and technical standards to be set for data protection by the regulators.

How do these turn into opportunities for the Netherlands?

India, under the leadership of Prime Minister Narendra Modi, has made Cyber Security a strategic priority, realizing the global position and enormous importance of the Information Technology (IT) industry for India's economy. The government has realized that, because of its vulnerability towards cyber-attacks and lack of awareness about Cyber Security in businesses and society, India could very well lose its market share in the global IT industry, if structural changes are not brought about at the earliest. The Netherlands has walked ahead of its time in this aspect, having rolled out a National Cyber Security Agenda (NCSA), enumerating the steps a government should take, to ensure a robust Cyber Security backbone for the country, which could, in turn, be helpful in the Indian context.

1. Policy and Regulation – The Netherlands has a rich tradition in open innovation and cooperation between businesses, government and research institutes to stimulate and accelerate entrepreneurship; the so called Triple Helix model, which can be successfully implemented in India, as the establishment of the Hyderabad

Cyber Security Cluster has shown. With a market as big as India, there is definitely more opportunities to create similar entities across the country.

2. Capacity Building both at government and industry –The Netherlands can help India in building and strengthening its Cyber Security infrastructure, develop expertise in the sector and apply its resources efficiently. India is witnessing a gap in the area of Cyber Security skills, as there is a dearth of trained manpower. This provides opportunities for the Dutch, as the Netherlands has a strong track record in training and capacity building in the field of Cyber Security.

3. Developing new products through R & D collaborations – the Netherlands and India can develop new products and services through strategic Research and Development (R&D) collaborations, that cater to the needs of both the countries.

4. Supply of products and services – In India there is a massive increase of online transactions and unsecured mobile phones. This has exposed banks and other financial institutions to significant waves of cyber attacks. Online fraud is on the rise, and the infrastructure is struggling to cope up with the sheer volume of online transactions. Dutch companies, with their state-of-the-art products and services can enter the market easily, providing the country with much needed tools to combat the challenges it faces.

5. Cyber Forensics – The Netherlands is amongst the best in the world in the area of Cyber Forensics. With a rise in the amount of cyber crimes, there is a need in India to develop its expertise in the field of cyber forensics. Dutch companies can help India in this aspect, thereby eliminating the need to reinvent the wheels.

Government initiatives in the Indian Cyber Security field

It was just 21 years ago that public internet came to India and currently India has the third largest number of internet users in the world, after the USA and China. With the recent government push towards a digital (cashless) economy, India is rapidly heading towards a Digital Society. This increasing dependency on digital technologies highlights the need for a secure cyber space in the country, especially when a number of users are novices as far as secure practices go.

The government has identified the following objectives for securing country's cyber space:

- Preventing cyber-attacks;
- Reducing national vulnerability to cyber-attacks; and

- Minimizing damage and recovery time from cyber-attacks.

The initiatives taken by the government of India have largely focused on threats to critical information infrastructure and national security, adoption of relevant security technologies, information security awareness, training and research. Due to dynamic nature of cyber threat scenario, these actions need to be continued, refined and strengthened from time to time. Various initiatives were simultaneously undertaken by the Government of India to address Cyber Security challenges, such as:

A specialized unit called the **Indian Computer Emergency Response Team (CERT-In)** has been operational as a national agency for Cyber Security incident response. It has been functional since 2004 and is actively involved with mitigating cybercrimes in India.

In 2008, the Government of India enacted the **Information Technology (Amendment) Act 2008,** to cater to the needs of national Cyber Security regime. This Act was later amended, to cover broader security related issues.

In addition to the above, a **National Cyber Security Policy** has been put in place in the year 2013.This policy was launched to integrate all the initiatives in the area of Cyber Security and to tackle the fast-changing nature of cybercrimes. Initiatives such as setting-up the **National Cyber Coordination Centre (NCCC), National Critical Information Infrastructure Protection Centre (NCIIPC)**, and creating sector specific **Computer Emergency Response Teams (CERT)** under CERT-In etc. were implemented under the above policy.

The Government of India has formulated a **National Crisis Management Plan** for tackling cyber-attacks and cyber terrorism. This plan is re-evaluated yearly and updated to tackle the changing landscape of cyber threats. Security Auditors have been empanelled for conducting security audits by both government and private companies.

Although the Government of India has passed laws and set up agencies, the onus is on the individual States to take up initiatives, drive on-ground implementation and ensure that a safe cyber space is created in the local environment. Hence, it becomes imperative for each State to adopt a dynamic approach to maintain a safe cyber space through effective and ever-evolving policies. The States of Telangana and Karnataka are the first in India to realize the importance of State driven initiatives in the sector and are leagues ahead of their compatriots in the country in terms of policies defined, activities undertaken, and infrastructure developed, in the field of Cyber Security.

Dutch footprint in Indian Cyber Security landscape

The Dutch Trade Network India (TNI) has played an active role in creating a platform for the Dutch companies in Cyber Security to enter the market quickly and efficiently. Leveraging on the growing ties between the Netherlands and India in politics, research and business, many high level visits have taken place between the countries and Memorandums of Understanding (MoU) been signed, with specific focus on Cyber Security.

In the year 2015, the Alderman of The Hague, along with a delegation of Cyber Security companies visited India. During the visit, the Municipality of The Hague signed a MoU with the Government of Telangana, to collaborate in the field of Cyber Security. The MoU enumerated various aspects of collaboration, such as providing trainings, Research & Development (R&D) support to various departments of the State of Telangana, assisting the State in critical information infrastructure protection, Government networks, e-Governance and Policy frameworks etc.

When the Alderman of The Hague visited India again in 2016, a MoU was concluded between the State of Karnataka and the Municipality of The Hague, which covered, *inter alia*, the topic of Cyber Security. One of the topics covered under the specific head of Cyber Security in the MoU was the creation of favourable opportunities for companies and training institutes from both the regions to establish themselves in each other's region. The MoU also provided for capacity building in Karnataka, in the field of Cyber Security.

Under the auspices of the MoU between the State of Telangana and the Municipality of The Hague, the State of Telangana has, in the year 2018, facilitated the formation of a Cyber Security cluster in Hyderabad called the Hyderabad Cyber Security Cluster (HCSC). This cluster, modelled after the famed triple helix model of The Hague Security Delta, is composed of Govt. entities, Knowledge Institutes and Private Sector companies, becoming the first Cyber Security cluster in this part of the world.

Following the successful establishment of the HCSC, The Hague Security Delta (HSD) and HCSC has, in May 2018, concluded a Program of Cooperation (PoC) in the presence of the Worshipful Mayor of The Hague, Ms. Pauline Krikke. This PoC has been concluded, *inter alia*, to strengthen the collaborations between The Hague and the State of Telangana in the fields of Cyber Security and technology development, related industries, and knowledge institutions.

During the visit of the Prime Minister of the Kingdom of the Netherlands to India in May 2018, a joint *communique* was released by the two Governments, enumerating the key topics for collaboration between the countries. This *communique* laid down the foundation for an ongoing, bilateral 'Cyber Dialogue' between the two countries, to discuss, *inter alia*, internet governance, data protection, Cyber Security policy, Computer Security Incident Response Team (CSIRT) co-operation and international capacity building. This India-Netherlands cyber dialogue is scheduled to take place in December 2018 in The Hague and will deepen the cooperation between the two countries on cyber-diplomacy.

An India – Netherlands Summer School for Indian students keen on Cyber Security was organized in The Hague, in the month of July, 2018. The participants got educated on cutting edge Cyber Security developments during a five-day programme, experiencing fascinating lectures by experts and professionals in the field, insiders' perspectives, exciting group challenges and opportunities to work on their social network. Five students from the State of Karnataka and six students from the State of Telangana were sent by the respective State Governments, to The Hague to attend the Summer School. Parallel sessions were organized in Hyderabad for a larger group of students, over the internet.

In August, 2018, K-Tech, the Cyber Security Centre of Excellence (CS-CoE) of the State of Karnataka, joined the Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity (Global EPIC) as its 24th partner globally and the first one in India. Global EPIC partners co-create and adopt world-changing solutions to high-impact cybersecurity challenges, both current and emergent. Underpinning this perspective is a conscious attempt to 'glocalize' – localize the global and globalize the local to generate economic development opportunities whilst simultaneously tackling cybersecurity issues.

In October 2018, a consortium of eleven Dutch Cyber Security companies, looking to enter the Indian market, was formed under the umbrella of the Dutch Government program – Partners in International Business (PiB). This PiB on Cyber Security, co-ordinated by the HSD, will, over the course of next four to five years, provide enhanced visibility to Dutch Cyber Security sector in India, create around EUR 21 mio in revenues and help the participating companies enter the Indian market with active support from the Dutch TNI. The Dutch Government has committed EUR 350k in support for the PiB, which would include incoming missions, seminars, economic diplomacy etc. It would be possible for other Dutch Cyber Security companies to join the PiB by complying with its membership requirements.

Key Cyber Security events in India

A wide variety of regional and domestic trade fairs are organized in India throughout the year in the field of Cyber Security. At several of these exhibitions, Netherlands Embassy and Netherlands Business Support Offices (NBSO) organize events, such as Holland pavilion and / or networking events.

a. **Cyber Security Conference**
Hotel Avasa, Hitech City Road, Madhapur, Hyderabad
4-5 December, 2018
http://kenes-exhibitions.com/cybersecurity/

b. **SecuTech India**
Bombay Convention & Exhibition Centre, Goregaon, Mumbai
25 – 27 April, 2019
http://secutechexpo.com/

c. **India's IT Security Expo and Conference**
Bombay Convention & Exhibition Centre, Goregaon, Mumbai
15-16 May, 2019
https://www.itsa-india.com/home

Key Market Associations

a. **The Information Systems Security Association (ISSA),** India Chapter, http://www.issa-india.org/
b. **Information Security Research Association**, India chapter, https://www.is-ra.org/chapters.html
c. **Cyber Society of India**, Chennai, India, https://cysi.in/
d. **National Association of Software and Services Companies** (NASSCOM), India, https://www.nasscom.in/

What can we offer?

Dutch Trade Network in India (TNI) has very good contacts with main market participants in the Cyber Security sector and also various regulatory authorities in India vis-à-vis Cyber Security industry. TNI offers active support to Dutch companies interested in doing business in India in finding potential clients / JV partners / participating in the trade fairs etc.

Contacts (More Information)

You can always contact us for more information at:

Netherlands Business Support Office, Hyderabad, Email: Hyderabad@nbso.info;

Netherlands Business Support Office, Ahmedabad, Email: Ahmedabad@nbso.info;

Economic Affairs Team, Embassy of the Kingdom of the Netherlands in India, New Delhi, Email: NDE-EA@minbuza.nl;

Consulate General of the Kingdom of the Netherlands, Bangalore, Email: BLR-EA@minbuza.nl;

Consulate General of the Kingdom of the Netherlands, Mumbai, Email: BOM-EA@minbuza.nl.

Colofon

Dit is een publicatie van:

Netherlands Business Support Office, Hyderabad, India

Contactpersoon:

Ajay Justin Odathekal, Trade & Investment Commissioner
Ram Babu Vedantham, Deputy Trade & Investment Commissioner
Hyderabad@nbso.info
+91 40 4203 0789

RVO.nl

De Rijksdienst voor Ondernemend Nederland (RVO.nl) is onderdeel van het ministerie van Economische Zaken. RVO.nl stimuleert ondernemers bij duurzaam, agrarisch, innovatief en internationaal ondernemen. Over de grens liggen vele mogelijkheden en kansen. RVO.nl begeleidt ondernemers met internationale ambitie bij het vinden van informatie over de exportmarkt. Ook helpen wij bij het leggen van contacten met zakenpartners en het benutten van (financiële) ondersteuning.

NBSO Hyderabad

Het NBSO-netwerk bestaat uit 20 kantoren in 10 landen. De kantoren zijn gevestigd in regio's die kansen bieden voor Nederlandse bedrijven, maar waar geen ambassade of consulaat aanwezig is. De NBSO's hebben een uitstekend regionaal netwerk. Hierdoor zijn zij in staat u snel de juiste informatie te leveren. Bovendien heeft het NBSO goede contacten met de overheid in het land. Het NBSO-netwerk wordt mogelijk gemaakt door RVO.nl en werkt nauw samen met de Nederlandse ambassades in het buitenland. Het NBSO in Hyderabad maakt integraal onderdeel uit van het Economisch Netwerk in India. Dit netwerk bestaat tevens bestaat uit de Nederlandse Ambassade te New Delhi, de Landbouwraad en de Netherlands Foreign Investment Agency.

Dit is een publicatie van:
Netherlands Business Support Office, Hyderabad, India.
Rijksdienst voor Ondernemend Nederland
Postbus 93144 2509 AC Den Haag
www.rvo.nl