CYBER SE
IND

VARINDIA organized a full day seminar on Cyber Security Framework; Securing FinTech Companies; Securing Smart Cities 1,000 Cyber Start-ups by 2025; and Strengthe

Kiren Rijiju, MoS for Home Affairs, Govt. of India delivering keynote address at Cyber Security India Conclave 2017

We all know that India is moving towards digital economy and we are going to face lots of challenges. Given the size of India and the nature of its society, lots of challenges stare us in the face. We may not have as robust a system as Israel or America because of the fact that the basic foundation of our country is slightly different and the structure of our nation is also a bit different. Nevertheless, the time is very crucial for us and we cannot lag behind in terms of understanding the challenges and the efforts to deal with the issues on hand.

We all know that our Prime Minister's effort and vision is very clear. We are talking about cashless economy and all related steps being taken by the Government will take us in a particular direction to accept the challenges and move ahead. We cannot achieve this alone in the government. We have to have all the private organizations integrated into our efforts at various levels and from all of the countries like Israel, America, etc. In recent times, whenever our Prime Minister or anybody from the government visits or exchanges some bilateral talks with friendly countries, the foremost understanding is on sharing of intelligence. This has become an integral part of any MoUs which we arrive at. Unless we share information with regard to various threats, security issues then the forging of partnership remains incomplete. The same reciprocal attitude has been seen from our friendly countries. The challenges are there for everybody so it has to be a combined effort.

India needs to secure its digital payments system by building its own cyber security framework to provide secure payment to its citizens and it is not an easy task.

In the Home Ministry, we keep on updating ourselves, but I could clearly see the challenges which are not going to be easy for all of us. This rapid development of digital technologies and a wide range of services provided for activities in the cyberspace raise the issue of cyber security as a serious concern for the government. Cybercrimes pose a direct threat to the security of critical infrastructure and information technologies.

With the advent of advanced information and communication technologies, crime now knows no jurisdiction or national boundaries. The very nature of internet allows for unprecedented collaboration and interaction among particular communities of criminals. As cybercrimes can be created at anytime in the world in an unprecedented way, it becomes extremely difficult to track, prosecute and enforce penalties. Therefore, criminals are increasingly turning to internet to facilitate their activities and maximize their efforts. Using cyber-attacks, terrorists can cause a much wider damage to the country or region than they could by resorting to conventional physical violence.

Government is aware of the vulnerability of information technologies. India is shifting gears by entering into the facet of e-Governance. India has already brought sectors like income tax, passport, visa under the realm of e-Governance. Sectors like police and judiciary have also planned to follow. We really need to update our policing system. The travel sector is also heavily relying on this. Most of the Indian banks have gone for full-scale computerization. This has also brought in concepts of e-Governance and e-Banking. The stock markets have also not remained behind. To create havoc in the country, these are lucrative targets to paralyze the economic and financial institutions. India has to cover a long road to make its cyber security effective. It has to cover a long road in cyber security initiatives and we are gaining momentum.

Contd. on pg 39

ECURITY
DIA CONCLAVE 2017

and focused on topics like: Building India's Cyber Security
s and IoT Devices; Creating One Mn Cyber Security Experts and
ening Data Protection and Cyber Security Laws

P.P. Chaudhary, MoS for Electronics & IT, Law & Justice, Govt. of India delivering keynote address at Cyber Security India Conclave 2017

Friends, through a series of path-breaking transformative initiatives, under the dynamic leadership of Prime Minister Narendra Modi, the country has taken giant strides to fast emerge as a digital economy and inclusive knowledge society. This also necessitates putting in place requisite infrastructure, mechanisms and process in place to fully secure our cyberspace from all possible cyber-attacks and cybercrimes as a pre-requisite and to keep our cyber defence in place. In this backdrop, I congratulate VARINDIA for organizing Cyber Security India Conclave 2017 which is both timely and relevant.

Friends, I wish to assure you all that the government is alive to ever-evolving dynamic security scenario since cyberspace has taken several proactive measures to create a digitally trustworthy economy. Under the overarching IT Act, 2000 as amended from time to time, a national cyber security framework is in place which takes on board all the stakeholders and cover perspective of secure cyber ecosystem, assurance and regulatory mechanisms 24X7, security operations, use of indigenous security technologies, workforce availability and development. Global cooperation and gap analysis with several countries, a national cyber security policy is already in place in the public domain.

Indian Computer Response Team (CERT-IN) has been operational on a 24x7 basis and all cyber security-related incidents are to be reported to CERT-IN. It works closely with affected entities and stakeholders both within and outside the country and provides initial response within four hours to a reported incident. CERT-IN undertakes activities of accessing the security posters of websites of sensitive organizations, particularly in the government, public financial sectors through both black box security audit and white box security audit. CERT-IN also empanels IT security auditing organizations which provide audit services on a commercial basis.

Cyber crisis management plan for countering cyber-attacks on cyber terrorism, periodically prepared by CERT-IN and approved by the national crisis management committee, is widely circulated amongst central ministry departments, states and union territory governments for implementation at various organizational levels. Regular workshops and drills are also organized by CERT-IN for various stakeholder organizations both in the public and private sectors.

The government has set up cyber forensics training and investigation labs at CBI academy and in the states of Kerala, Jammu & Kashmir and seven North-Eastern states of Assam, Arunachal, Meghalaya, Manipur, Mizoram, Nagaland, Tripura for training law-enforcement agencies and judiciary in these states. The CERT-IN cyber forensic lab also provides its services to law- enforcement agencies, state and union territory governments, PSUs, etc in the investigation of cyber security incidents and cybercrimes.

Setting up of a national cyber coordination centre under CERT-IN is in progression which would enable to anticipate and prepare to counter cyber-attacks and to generate cyber security situational awareness. An expert panel has been set up to recommend the changes required in the existing laws such as IT Act, criminal procedures, Evidence Act and IPC to plug the gaps, if any, in tackling the various forms of cybercrimes.

In the wake of historical demonetization drive which took place in the country recently, digital payments have shown exponential growth and hence Finance Minister Arun Jaitley has announced that cyber security is critical for safeguarding the integrity and stability of our financial sector. A computer emergency response team for our financial sector will be established. This entity will work in close coordination with all financial sector regulators and other stakeholders. The government has taken several initiatives and measures to safeguard and secure our cyberspace and digital transactions.

Session I: Building India's Cyber Security Framework

From L to R: **Eric Loit**, Chief Systems Architect, RAN International; **Marc Kahlberg**, CEO, Vital Intelligence Group, Israel; **Deepak Sahu**, Chief Editor, VARINDIA; **Deepak Kumar Rath**, Editor, Uday India; **Rama Vedashree**, CEO, DSCI; **Hemal Patel**, Senior VP-India Operations, Sophos; **Atul Gupta**, Partner-Cyber Security Services, KPMG; and **Dhiraj Gaur**, Technical Lead (Govt., Defense and ICS Solutions), Check Point Software Technologies

Marc Kahlberg: I managed to stop crime in 2002 in Israel by 70 per cent by implementing physical security concept which we call the secure zone or safe city. The cyber people of the world called it smart city. It is time to change as we are moving forward and we have to be aware. We have to work together to create a stop to the war that is going on in the cyberspace today. If you do not work together, nothing is going to happen. We have to encourage and cooperate between ourselves. We have to work together to create a platform of security.

We have created and developed a couple of frameworks for cyber security. In the six Ps of cyber security, the primary concern is the threat, the provision of education and awareness, protection; preventative measures are necessary; predictive measures need to be proactive. There are long-term challenges. The tasks we have to take up to make these challenges a reality. Cyber security is all about intelligence and the best form of defence is a good offence.

Rama Vedashree: It is a well-known fact that India is a powerhouse of Information Technology. India's advantage in cyber security is a well-kept secret because most global corporations which invest in cyber security centres of excellence or security operation centres or network operation centres do not usually advertise that capability and in which location it is. So we are beginning to feel that India during the last three years has become a chosen destination for security operation centres for a number of global corporations. Similarly, all industry members, whether it is HCL, TCS or Infosys, have very mature cyber security practices. We are also seeing companies like KPMG building capabilities in India for cyber security consulting and services to be able to deliver to the global clients. While it is a nascent industry, we are beginning to become a hub for innovation and product development.

We are looking at security R&D. A number of global corporations like Symantec, FireEye, EMC and RSA have chosen India as an R&D centre. According to our estimate, there are around 150,000 people working in their professional capacity in the overall information security and cyber security domain.

Hemal Patel: Cyber security framework consists of two things. One is definitely protecting our own assets in the country and building a leadership to promote cyber security products and services. Cybercriminals will always be ahead. Therefore, there will always be a data breach, cybercrime and data thefts. It is important for organizations or country to make sure how fast we can catch cyber terrorists and how fast we can respond to and how we can slow them down. Focussing on these three principles, if I have to build the cyber security framework to protect our own country's asset. I don't think there is a framework in the police force to record those events.

One of the definite things government needs to strengthen is the patent office. Second, we need to have a lab to certify our products and we are the only odd country where the government has the lab and it should be privatized.

Dhiraj Gaur: Digital initiatives which the Government has taken are touching lives now. We are entering an era where we are talking publicly about available internet, universal acceptance to technology, IT jobs for everyone, e-Kranti situations where we are touching the lives of farmers, e-governance initiatives which are very well can be seen in every state and every state is competing with each other. So having this digitization is very good but at the same time it has a lot of IT components and automation involved in it. In this era of transformation, one important thing which we have seen is that the mobile phones are taking over desktops. We have also seen that social scenarios are beating the search engines. Messaging apps are challenging the usual way of communication. Everything around us is becoming connected.

With the right architecture, the right strategy and having a thought process of staying one step ahead of the security advisory that should be our key approach to build a resilient cyber security framework.

Atul Gupta: In the last presentation, it was mentioned that 3.2 million debit card hacks happened in India. So there is a need today for us to have a robust framework. While talking about the good practices, the point goes back to awareness. I bring three elements around it. It is not just awareness. It is also making sure that you have the right skills and that is the bigger challenge today because making sure that skills are available to address cyber security effectively is a huge issue which we are facing as a country. The second area where we need to focus upon is competence and many times it gets interpreted as technology-related risk. I put it differently. It is a risk which has started because of technology but does not stop over there, but the challenge which comes when we start looking at technology which is changing at a fast pace.

Deepak Kumar Rath: In India, cybercrimes come under the Indian Penal Code and the IT Act, 2000 which was amended in 2008. Since policing is a matter of state and complaints have to be lodged with the police, it all depends under the law that police register a case. It so happens that for most of the parts they prefer the age-old Indian Penal Code (IPC).

Local police are not conversant with the intricacies of the IT Act. But once a case is filed under IPC, the method of investigation must follow certain guidelines that make it extremely difficult to prove most cybercrimes, according to experts.

Session II: Securing FinTech Companies

From L to R: **Pravin Prashant**, Consulting Editor, VARINDIA; **K.B. Lal**, Advisor, Information Security, Oxigen Services; **Prem K Gurnani**, DGM-SOC, State Bank of India; **Arvind Gupta**, National Technology Head, Bhartiya Janata Party; **Carmit Yadin**, CISO and Director of Cyber Division, Vital Intelligence Group; **Puneet Kaur kohli**, EVP - IT & Group CTO, Bajaj Capital; and **Gurpal Singh**, Sr. Market Analyst, IDC CCR India

Arvind Gupta: In the budget, digital economy was a special section and the Finance Minister has announced CERT for banks. The digital should be the norm and the cash should be the exception.

The banks and the network layer need to be secure. We don't concentrate on use, app and instrument they use. If the consumers would have adhered to cyber hygiene, people would have saved around Rs.3,700 crore. The importance of mobile PIN is to get people digitally literate. So one needs to educate people on financial literacy. During demonetization, the highest number of requests for banks was I do not know my PIN number.

In the BHIM app, the app layer is also secure. If you install an app, it requires 20 permissions. BHIM app is a standard app where the user, app, mobile phone, network, and server is planned in a holistic way. In the FinTech companies, all these parameters are very critical.

During demonetization, the E-wallet transactions increased in November and December, whereas in January these remained stable. In IMPS transactions, it peaked in December and January, whereas in the case of BHIM/UPI app, the transactions have increased from Rs.90 crore to Rs.1,270 crore and are competing with all the wallets combined.

The biggest challenge for FinTech companies is to make digital transactions secure and India is leading the world in FinTech revolution globally.

Prem K. Gurnani: I am quoting a news story about millions of cards being blocked and SBI was mentioned in the headlines. We got calls from all over law-enforcement agencies and all regulators but what was the instance. It was a non-SBI company, a particular bank which had outsourced some activity to a particular service provider. SBI has the largest customer base, largest card base and nothing has happened in SBI. What I am trying to highlight is that being a leader has its own challenges.

SBI, a couple of years back, has outsourced law monitoring security operations but depending upon the volumes we do not permit setting up logs outside. So, we set up our own security operations centre (SOC) and this environment is helping the banks.

In 2011, RBI came out with the guidelines on information security which mandate banks for governance structure, IS Security, and CISO report to the management. On 2nd June, 2016, RBI came out with cyber security for banks with another list of activities which include: CERT-IN audits, cyber drills, NCIPC pitching, RABBIT, and opting of cyber security professionals. The ecosystem is converging and facilitating security for Buddy.

Products need to be rolled out fast, but unless these are tested by the security team and a clearance is given, the products cannot be rolled out. You would see many times that SBI is not the first to roll out a product to hit the market.

SBI has a strong security team taking care of products, a strong governance structure, strong awareness about customers and staff programme in place.

We manage traffic as well as security and since it is SBI we see attacks every day – be it phishing attacks, DoS attacks and DDoS attacks at a regular frequency. Investigative measures are in place at the network layer, application layer and transaction layer.

With transactions going up now, there is a separate set-up for monitoring transactions to alert customers whenever there is any suspicion.

K.B. Lal: Oxigen started in 2004 and the initial objective was to perform digital operations like mobile recharge, DTH and bill collection. When we want to assure our customers, we have to look at external threats as well as internal threats. We want to assure the customers and we want to make it easy.

Wallet has a six-digit password and has a two factor authentication but the customer does not want it.

Cyber security has a two dimension perspetive. Defensive provides comprehensive vulnerability and is somewhat protected from attacks. On the preventive side, train our partners and designers to use secure coding guidelines formalized structure within the government. The focus is also on third-party audit or ISO 27001. This is all endless as cyber security is a continuous effort and we have to keep on improving.

Puneet Kaur Kohli: FinTech industry needs to be digital savvy. We have taken an internal landmark where we will wait to have ISO 27001. It is not about IT security but enterprise level security. How consistent are we in terms of leveraging the certification and then utilizing the adoption and cultural change within the organization and regulated by IRDA and SEBI. One set of rules and regulations is not enough.

Carmit Yadin: On cyber security, there are three main factors:

1. It is interesting time for India as it is going digital. How India is going to protect the biometrical database? Every person is going to get digital identity to manage his financial assets and the government needs to provide robust cyber security infrastructure on this asset. No one will change his fingerprint. How the government is going to protect people. If this information is leaked, financial information can be broken.

2. Awareness and education must be in place for the entire nation. Everybody has to understand the risk and needs to know how to avoid risk.

3. India has taken dramatic steps in this financial digital world. It also became very attractive targets to hackers and enemies and everyone wants to put a hand on these critical assets and the way I see and working with different governments in the world now it is right time for India to build a strong robust cyber intelligence methodologies and create cyber intelligence infrastructure.

These are very interesting and important and how it looks from outside. India will be a secure nation. Whether India will be a secure nation or will India lead this industry and create standard. All countries around India will learn from India.

Arvind Gupta: Our inspiration has been defined by our Prime Minister. We want to do innovations for the next six billion. We are

technically an advanced superpower with one million engineers produced every year. The geopolitical situation we are in the world trust leaders. six billion grossly ignored because of the cost. All platforms have cyber security to the world.

Gurpal Singh: Four mantras. First, for any organization, security infrastructure can be very expensive. Seocnd, if they don't have architecture for the product ingrained by design and not as an afterthought as an interface. When you are writing the first code all the developers should have that piece. Third, what security tools are using to identify and access management two factor authentication, privilege access management, encryption tools. Recently, CERT advised banks and NBFCs to have strong encryption capabilities. Every point your database, every point your mail, every point your product and that ownership lies with lot of Fintech companies. Regular third-party audits to access your security. Managing internal risk comes from advice and third-party suppliers and contractors.

Lastly, FinTech what kind of SLAs they have from the government bodies. The average lag time is 14 days in the production system. Post demonetization, FinTech companies got the scale but also got a lot of vulnerabilities in the ecosystem. So there is a need for establishing a regulatory authority for digital wallets.

Session III: Securing Smart Cities and IoT Devices

From L to R: **Pravin Prashant**, Consulting Editor, VARINDIA; **Brijesh Singh**, Inspector General of Police (Cyber), Maharashtra Police; **Purushottam Kaushik**, Sr. Advisor- Smart Cities and Infrastructure, McKinsey India; **Shree Parthasarathy**, National Leader- Cyber Risk Services, Deloitte; **Rajnish Gupta**, Sales Director, RSA India; **Vipin Tyagi**, Executive Director, C-DOT; **Samir Datt**, Founder & CEO, Foundation Futuristic Technologies; **Pankaj Kumar Gupta**, OSD, Strategy, Business Growth & Operations, (n) Code Solutions (A Division of GNFC); and **Ajay Purohit**, Sr. Vice President, Fourth Dimension Solutions

Brijesh Singh: More than a policy question, it is about technology question when you look at IoT. It does not have enterprise security like protected firewall, IDS/IPS, Flow Analysis, Malware analysis and endpoint protection.

I think security for IoT devices is not very developed still and it would need much better solutions.

The IoT devices have very aggressive power management and they do not have an operating system and they are liable and susceptible to any kind of attacks. Surely, all this infrastructure is outside as the threat surface area is very, very large. So threat of IoT devices and smart cities is more like a technology challenge than a policy challenge and I hope we will have to find a better solution in the times to come.

Pankaj Kumar Gupta: Gandhinagar became the first operational city a month back. It is much more than a regular CCTV as our Wi-Fi system has 15,000 concurrent users having about 2 Mbps and about 30 minutes free Wi-Fi usage. Gandhinagar smart city also has smart sensor-driven street lights, environmental sensors and many other components.

Technologies can be executed, but the big question is how secure are they. We have conducted 26 tests before we launched this project. The project was executed in about three months and it took four months to fix those gaps through 26 tests.

I think we have security which needs to be implemented. IoT sensors are a very good technology. If implemented properly, they can definitely deliver results. And I can assure you as a consultant to Gandhinagar smart city, implementation is 100-per cent secure.

Vipin Tyagi: What we have missed in smart city is design. The open platform has not been adopted as the focus is on the proprietary platform. Smart city requires an integrated IP-based core network and then you require applications.

30 per cent of the total traffic flow on Internet is BOT or BOT-like. Attacks are large-scale vectors or multi-vectors. How standardization will build security?

Tower Monitoring Site (TMS) is a nationwide public infrastructure and it has to be secured. We need to have a standard-based platform where everybody can connect. With respect to blast, law-enforcement agencies need to be fully equipped as they can trace where was the machine, who did it, at what time the command was actuated, at what time did the detonator go and its likely impact.

Purushottam Kaushik: In smart cities, everything will become smarter. The challenge is all the pieces of smart city whether the endpoint which is in the streets or closer to your home and whether it is the gateway which is carrying the data network or central piece or command and control or maybe the data layer the exposure point is everywhere whether it is touched or played. The impact can be huge. Presently, we are not smart so we are not exposed. When everything gets connected, it is not too much of an effort to switch off the lights of the whole city. It does not take too much of an effort to keep playing with the transparent system of the city. That is where the big time impact or exposure can happen.

Presently, smart cities are in silos. Somebody is focussing on Wi-Fi transport solutions, integrated traffic management, waste bin deployment or smart parking. All these projects are executed in silos as there is no framework or plan and how it will get integrated with smart city. As a technology leader, we will focus on how do we build silos around smart city. Now perhaps from the consulting point of view unless we look at it holistically, we will not be able to solve it whether we build a framework of security across the layers or on the services perspective as we move forward and how do we manage security on a day-to-day basis.

We need to have continuous security layer on every piece at all exposure points. We need to build a services layer perspective. Any of these smart cities put a layer on top of it where we are going to have a third-party practice of analyzing each and every security layer. Certifying and auditing it after every three months will help us to be proactive.

Shree Parthasarathy: We have involved from generation to generation, there are a lot of expectations from a fundamental city. As we are tagging a smart city, the expectations of the common citizens are just going to go up.

ATM, which is a trusted network so far,

the expectation was I go to my ATM and put my card and I will get money. For two months, ATM was out of order and the machine was not working. Let me take related services from the smart city perspective. So when you have the same expectation and when you look at security, you focus on confidentiality, integrity, availability and privacy of information. Once we get information about citizens, how do we ensure privacy of information.

The second is availability and the biggest challenge facing the IoT industry is end sensor and power in the end sensor. IoT manufacturers are facing how to make it economically more viable and second how to maintain the power and third is how do you embed security in every layer.

How to embed security to the sensor level all the way to data layer and how do you do that?

The availability of sensor is significantly important as there is a reliance on sensor providing critical information and that goes into service layer and services and availability of sensor at that point is very critical.

All these cities need to talk to each other in a very secure fashion and also the integrity of the data flow needs to be together.

The last area is confidentiality and how it is managed? If you look at a smart city, you have government, you have a service provider, you have a number of organizations like us creating RFP, project plan, business plan, then you have technology providers. What is important is common framework, standards for a set of smart cities need to be consistent.

Samir Datt: Let us go ahead 20 years into the future where artificial intelligence is speaking to each other. I think we are living in very revolutionary times where things are changing dramatically. Networks are getting heavily interconnected, standards exist and in the implementation of those standards there is a lot of gap. We talk about IoT, but any chain is as strong as the weakest link. Even if there is one device or one system that does not conform, you can bring the whole network down. What do we need to do?

There was a movie – Live Free or Die Hard. In the movie, they hacked everything right from street lights, TV channels, cell phone networks, parking networks, communication between underground metros, underground-to-air network, electricity grid and even nuclear facility. We need to look at three important things – People, Process and Technology and we need to have smart people.

Ajay Purohit: Managing the expectations of the clients – multi-technology, multi-vendor and multi-process the big question is will OEMs follow standards as they have their own proprietary technology and are they interested in interoperability. There is a big question mark on that. The only way to ensure such things going forward is to ensure by bringing in regulations or bringing standard frameworks. Presently, we do not have the capital outlay where you can go for 100- per cent smart city. The project will come in phases. So how will you ensure that when they are coming in phases they are all integrated. The bigger question is even if it is integrated, there is a technology shelf life. By the time you reach phase III, phase I technology is due for overhaul. So there has to be a policy in place on how a technology is evaluated, inducted, procured, implemented and then phased out.

Unless and until these frameworks come into place, you will always have these models. A plethora of devices and a plethora of networks are all talking to each other but not making it secure.

Rajnish Gupta: Smart City is like an enterprise. You have an endpoint, you have a network there is an application and there is data. Smart city is an enterprise and what we do in an enterprise is to educate our users and administrators to manage the entire security which is the biggest thing. The government and regulators have the responsibility to manage the sensor providers technology and they need to follow standards. Unless we follow the standard, we will get security breach points. The standard could be authorization, encryption, authentication and what can be done and how it can be embedded.

Security is becoming a boardroom discussion. If we imbibe the security piece at the conceptual level, it becomes much more easier to roll out. If we roll out and then try to do this, we will never meet that. Sectoral CERT has come right now. We have to set up the governance model and how to mitigate the risk.

How do we see what is happening on the network? How do we see what is happening on endpoint as they are most vulnerable? Most attacks come from endpoint. Look at the vendors who give security as a preference, people who are making devices with more secure infrastructure in the component.

Brijesh Singh: Our cyber security project is conceptualized by our Chief Minister and it is a Rs.1,000-crore project. First, technology assisted investigation for police. Second, Maharashtra will have its own CERT which will be state-of-the-art. Third, bring data analytics platform to be used by law-enforcement agencies. Fourth, a large awareness programme for people at large.

Maharashtra has already formed one cyber police station per district. So presently it has 44 cyber police stations. It has the latest state-of-the-art tools, technologies and training. We are taking manpower from outside. We are taking people from the market at market rates so that we are not constrained by not having proper staff. Though it is experimental, we have had a fair amount of success.

We will have CERT in the next six months, followed by Big Data platform and very soon threat intelligence sharing platform. Other states have evinced interest as to how Maharashtra is doing it and if we are able to do it, it will increase the confidence of investors that you have a robust cyber infrastructure in Maharashtra and Mumbai and that would in turn help Maharashtra to be a good destination for investment.

Pankaj Kumar Gupta: Please don't buy devices or equipment, but please buy outcomes. Gandhinagar Smart City RFP talks about what I need and what is the outcome. It is based on the Design-Build-Own-and-Transfer model. The security audit is conducted every three months, thereby improving the system and replacing the system.

Shree Parthasarathy: As we move into the digital age and as we bring everything digital and everything online, the big question is how we adopt them and implement them across all layers and put right level of governance and risk management plans.

Session IV: Creating One Mn Cyber Security Experts and 1,000 Cyber Start-ups by 2025

From L to R: **Amajit Gupta**, ICT Expert & Angel Investor; **Rohit Srivastwa**, Senior Director (Cyber Security & Education), Quick Heal; **Shrikant Sinha**, CEO, Nasscom Foundation; **Debabrata Nayak**, Chief Security Officer, Huawei India; **Dinesh Pillai**, CEO, Mahindra Special Services Group; **Harold D'Costa**, CEO, Intelligent Quotient Security System; and **Trishneet Arora**, CEO, TAC Security

Amajit Gupta: Definition of cyber security in terms of shapes and sizes and where is the money? I think national cyber security is getting more and more profound. It is the early stage industry. Like we do it in India one way, i.e. Jugaad. We find the size and shape to our story as we go along. We see a national vision from NASSCOM and DSCI of one million cyber security experts by 2025, but when we look at the drill you have missed the number by a factor of six times. The nearest number we need to train in this country is 6.5 million every year and that is cyber security awareness. The rest is IT initiated who need to be trained for cyber security are the software and the service providers and that market is 1-1.5 million professionals.

What is the state on the supply side? On the supply side, only about 20,000 cyber security professionals of the IT kind churn out every year or may be even lesser.

Rohit Srivastwa: We are a start-up in cyber security and was acquired by QuickHeal. We are on the education side called QuickHeal Academy where we are designing the course curriculum for M.Tech in Cyber Security with the help of industry experts. We have signed an MoU with Gujarat Forensic Sciences University and Chitkara University. The focus is on converting the educated into employable in the cyber security space.

Debabrata Nayak: For Huawei, it is do or die. There is no budget listed for cyber security. We have 160 cyber security professionals for thorough testing of equipments. Autonomous institutes can bring cyber security courses for B.Tech, M.Tech and Ph.D. This time, budget talks about cyber security. Institutions can bring cyber security courses and then train cyber security professionals.

Dinesh Pillai: As an end-user, we do not follow basic hygiene. Technology shift will be there, but there is only one thing which is constant is people. We have to do a reality check with respect to training on cyber security. Who is going to teach? People who have done CCNS come and say I am a cyber security expert.

What is the basic definition of cyber security. I am an expert in information security and not cyber security.

Who is going to train? Who is going to accredit as cyber security course labs come at an exorbitant cost.

Harold D'Costa: In 2006, diploma in cyber security in Maharashtra top universities was not the right time. Nashik University said yes to me for Diploma in Cyber Security and there were 101 admissions. 93 sat for the exam and 62 cleared. 25 per cent left the country and are serving in other places. Maharashtra Police Academy has launched a 3-day training programme for corporates to tell what the police is doing on cyber security from both the technical and legal side. In Nashik, there are 5,000–6,000 industries and Nashik Police will train corporates on cyber security.

As to training the judicial system, where are the people? As far as the government is concerned, there are 5,060 professionals in the government system. In 2012, AICTE sent circulars to all universities to start a mandatory course on cyber security. Many of the teachers who came from hardware were teaching cyber security. The big question was where are the people to teach cyber security? Build cyber security research cell where the government can introduce – and we will give them jobs and we will absorb them. Time has come for more action, more training and then absorb them at the earliest.

Trishneet Arora: We are not empanelled even after four years. If we are not empanelled, how will you get 1 million ethical cyber security hackers.

In 2011, NASSCOM talked about 77,000 ethical hackers every year. How many you have got till 2016? A number of institutions provide 6-week and 6-month courses but they don't know the commands. They are producing donkeys. We will have to get government empanelment. Otherwise, nothing is going to happen. We are fighting with young criminals. So how a 50-year-old man is going to fight with a 15-year-old kid. If I am fighting, I believe a lot of young start-ups are also fighting. We are testing financial institutions and banks.

Dinesh Pillai: To manage 80,000 people, there are 8 people in the info security team and this bank is of national importance. 8 network and administrators moved to the security cell. If an attack happens, they would not be able to manage it.

Amajit Gupta: We have to target large IT experts as government cannot comprehend the problems. Supply vendor relationship will destroy your business. Talent is over here, but we don't have the environment to grow. I would urge upon large corporates to put money where the mouth is. For private risk ventures, cyber security should be a priority.

Dinesh Pillai: The industry has enough challenges to address and there is scarcity of people. Many times, somebody has to do accreditation. The accreditation has to be done by government agencies.

Rohit Srivastwa: The industry has to teach as real knowledge will come when the industry teaches.

Trishneet Arora: We have students for industrial training and I think this is the only way to train resources. Cyber security is a business issue and not a technology issue. It is a business risk and we should give chance to cyber security start-ups so that they can come up.

Who will train? An agency which should certify people. They in turn should train the trainers or professors and professors then should train the students.

Session V: Strengthening Data Protection and Cyber Security Laws

From L to R: **Pravin Prashant**, Consulting Editor, VARINDIA; **Rajat Chand**, Managing Director, CSDC India; **Samir S. Kanthale**, Joint Director, Judicial Officer's Training Institute, Nagpur; **Anil Dhawas**, Civil Judge Senior Division & Additional Chief Judicial Magistrate Daryapur, Dist. Amravati, Maharashtra; **Deepak Maheshwari**, Director - Government Affairs, India & ASEAN, Symantec; **Harmeet Kalra**, Head – Alliance, F5 Networks; **Amit Malhotra**, VP Sales-India & MEA, Seclore Technologies; **Harold D'Costa**, CEO, Intelligent Quotient Security System; **Keerti Nileish Mahajan**, Professor, Bharati Vidyapeeth University; and **Anyesh Roy**, Deputy Commissioner of Police (cyber cell), Delhi Police

Anil Dhawas: As a policy matter, the Government of India has announced digitalization of so many things, including digital payment, digital transaction, etc. Day in and day out, we come across digital evidence. Whatever we do electronically, we have to keeps digital footprints. Therefore, in fact, it is easy to catch the person who did digital transaction including commercial transaction or any crime.

As far as privacy is concerned, I believe the privacy of the people is at risk. Some measures have already been taken by the government by enacting the Information Technology Act. Some measures have been taken by framing rules under the IT Act. My basic question is: Are these rules sufficient and enough to protect the citizens from vulnerability of cyber incidents?

If a cyber incident occurs, the victim has to move from pillar to post. We have no specialized police in the requisite number; nor do we have specialized courts and judges trained in this field of knowledge. There is no uniformity in the courts with regard to the proof of digital evidence. There is an issue of jurisdiction, etc. For all such reasons amongst others, we need a uniform operating procedure to be followed by the courts.

In the government sector, every department has its own manual. For instance, in Maharashtra, for police department, there are police manuals for courts and there are civil and criminal manuals, but there is no manual in respect of the use of digital matters. Recently, the Income- Tax Department has launched its own manual for investigation in respect of digital evidence. So whenever any income tax official has to do anything he has to follow the guidelines of the said manual. But there is no manual in other departments. The necessary manual needs to be brought into force regarding digital evidence in order to bring uniformity. There is no provision in the manual of any state police. Hence, such manuals are needed for proper guidance for the police department.

There are rules framed in the year 2011 under the Information Technology Act in respect of the protection of privacy of citizens. The rules are not properly implemented. Surprisingly, what if those rules are violated? There is no punishment provided for the breach of the rules. How there would be deterrence in the minds of people unless there is provisions for imprisonment. If any victim sustains any loss due to cyber incident, what penalty is provided under the IT Act? Surprisingly, it is up to Rs.25,000. This is not a penalty, but it is a compensation by the person who supplies or shares the private information by committing the breach of rules. If the victims has sustained more loss, then such an amount of compensation is very meagre. Moreover, in order to get that amount of Rs.25,000, the victim has to approach to the adjudication officer. Anyway, where is this office? The adjudication officer sits in the state capital. For example, in the state of Maharashtra, the office of the adjudication officer is at Mumbai, for West Bengal, the adjudication officer is at Kolkata. Do you expect the victim to go to the state capital for seeking the meagre amount of compensation? Why can't you provide such powers of adjudication to the court at district places. Therefore, we need to revisit this provision and we need to amend the law.

Proving electronic record is a difficult task. Recently in the year 2014, the Supreme Court laid down a law that every electronic record must be accompanied with a certificate as contemplated under Section 65-B of the Indian Evidence Act. Therefore, it becomes mandatory to have such certificate whenever any electronic record is to be proved. I feel that this judgment has made the prosecution very difficult to prove electronic record. It has also brought difficulties in proving electronic evidence in civil cases. Nowadays, in every case such question of electronic record comes. Unless there is a certificate, no electronic record including CD, DVD or computer printout can be admissible as evidence. In many cases, there was no such certificate. The fate of such cases is going to be culminated in acquittal, particularly criminal cases in which the question of electronic evidence is there. The certificate is now mandatory. But is it practicable to furnish such certificate all the time? I wish to give an example. If you go to a petrol pump and fill up the petrol, you pay the money by your card. The moment card is swapped, one will get a bill generated electronically. If something happens with regard to quality of petrol and if you are required to file a case, then you need to have a certificate duly issued by the petrol vendor. Do you expect a petrol pump man who fills up petrol would be issuing a certificate to every customer? Is it possible for him? Will he fill the petrol or issue the certificate? But the law says you must have a certificate. This is something illogical and absurd. Hence, we need to relook at the Information Technology Act and the relevant provisions of the Indian Evidence Act. For every minor printout, why a certificate should be made compulsory which is not practical? Hence, we need to change the law. An amendment in the Evidence Act has become necessary.

After the Supreme Court's judgment in the year 2014, the Government should have done something. The Government could have amended the provisions of Section 65-B or could have provided some provisions into the said section by enacting an amendment or by promulgating an ordinance. But the Government did not do anything. It is so because there is no will to do so.

Mere passing stringent laws will not be sufficient. We need to educate the people from being protected from cyber incidents. Digital literacy is the need of the hour. We need to educate the people as to how to be secured in the cyberspace. What precautions should be taken, etc. I feel the Government should form a committee consisting of technical and legal experts to amend the law of electronic record and cyber security.

Anyesh Roy: Very few police officials have manuals or standard operating procedures or standing instructions for collection of electronic evidence. We have recently framed a standing order for collection of electronic evidence that covers desktop, laptop and mobile phone and other basics on sources of digital evidence. Most of the organizations don't have it. Even if they have it, it does not percolate to the investigating officer as they are very reckless in collecting electronic evidence and at the trial stage it may lead to acquittal and serious implications. The third issue is 65-B certificate. Even the courts are not updated about the provisions and the lower courts are not insisting on 65-B certificate at the initial stage. When cognizance is taken and charges are being framed but when it comes to the trial, the defence lawyer will rake up this issue, particularly after the judgement of Supreme Court in this regard. So these are the issues which need to be addressed and loopholes need to be plugged and only then the effective law enforcement will happen vis-a-vis cyber offences.

Release of Cyber Security Handbook 2017 by P.P. Chaudhary, MoS for Electronics & IT, Law & Justice, Govt. of India

Pavan Duggal: India doesn't have a cyber security law in force. If you want to look at the Indian Information Technology law as cyber security law you would be disappointed. You can't blame the lawmaker as the law was framed in 2000 and cyber security was nowhere on the horizon. We amended it in 2008 and cyber security had arrived but it was still not important and we have not amended the law. Bu the law in the present-day scenario is a sitting duck.

As a nation, we are not prepared should a cyber-attack takes place in India. It would be a

A view of stalls at Cyber Security India Conclave 2017

few hours before we surrender that's the current level of preparedness.

In this scenario, you need to have adequate first and foremost legal frameworks and we need to know what is happening across the world. There is laxity in our approach, whereas China during the last 18 months has come up with two important legislations – one on national security and the other on cyber security. The law is not only applicable to not just entire China, entire Internet but outside space.

The new concept of cyber sovereignty and what is India's position on cyber sovereignty? India doesn't have a stated position on cyber security. It is time we go beyond the paradigm of the IT Act.

The IT Act is good when we began; it was a small legislation. When we amended it in the year 2008, we transformed small legislation to biggest omnipotent mother legislation with data and information in the electronic form. But we now incorporating communications device and computer resources, this law has become one of the three most significant pieces of information – the ther two being Indian Constitution and Indian Penal Code. India needs an independent Cyber Security Law independent of the IT Act.

As a nation, we are unprepared tomorrow if our critical information infrastructure is attacked. We cannot afford to fight against the entire gamut of warfare agent critical infrastructure.

Cyber terrorists are structuring their activities in such a manner that their activities cannot be brought under Section 6- F of the Information technology Act. As a nation, I am quite clear that India cannot fight cyber terrorism with one single provision. We need to have extensive legal provision for judiciary and law-enforcement agencies.

It is time to revisit the law. It is time we need to do lot of capacity building. It is time when to come up with capacity deterrence and or states IT Act. We need to have cybercrime courts as cybercrime is happening all across the world. Cyber is centre to a variety of things. In 2017, my guesstimate is that 3 out of 5 cases require electronic evidence. It is time we revisit the rules for mobile evidence and who is going to give the certificate.

According to a report, the global cost of cybercrime is going to exceed $2 trillion. According to Forbes, 80 per cent of cybercrime is done by organized crime.

Keerti Nileish Mahajan: It is teacher's responsibility for creating new leaders. We have to cover all aspects in 1-year, 2-year or 3-year programme. We have to arrange skill development for students for short-term courses. In Bharti Vidyapeeth, we have Legal Aid Centre, where we are getting lots of cases. We give legal advice to students for such kinds of cases and we are giving compulsory cyber security to all students. Around one lakh students in Bharti Vidyapeeth and students need to get compulsory cyber security certificates for getting degrees.

Samir S. Kanthale: There are two things – awareness and capacity building. Maharashtra is the only state which has assigned training of public prosecutors. A question often arises if it is so technical, how do we deal with it. When we studied LL.B., this law was never in existence. It is not an easy task to try somebody who is an expert in IT before a court which has knowledge of the said subject. The Cyber Security Policy of 2011 has specifically dedicated state-of-the-art facility for cybercrime investigation and dedicated state-of-the-art training facility for law- enforcement agencies and judiciaries. Unfortunately, it is yet to see the light of the day. As an incharge of the training institute, I am requesting cyber security experts to come and enlighten our prosecutors on the subject.

When these cases are tried before the Supreme Court, we have just 65, but we don't have separate rules for investigation and acceptability of evidence. We need to have standard investigation procedures recognized by law.

The second thing is awareness. Even as a common man, we are hardly bothered about personal information pilfered or being misused. As a case-study, we studied the privacy policy of bank and we found that the privacy policy is indeed in a way to favour the banks, although prior permission is required to share the data with third party. I doubt whether this policy has been challenged at an appropriate authority.

Another issue, I would like to highlight is the availability of free or paid app on the App store. This is totally unregulated area and I believe there needs to be some authority to regulate, certify subscriptions of apps.

Deepak Maheswari: The IT Act is at the central level. Otherwise, we would have a central legislation as well as a state legislation. Notwithstanding that, we do have National Cyber Security Policy, 2013 much before that IT Policy in 2012, but many states had the IT Policy right from 1997.

Our policies have to be at least consistent and to be globally harmonized and even in the country it needs to be harmonized.

On the encryption part, on 7th August, 1999 we had 40-bit encryption, but what is the situation today? We have different types of provisions within different regulations. In online trading there are three different provisions and it is incompatible with one another. We do need to have a consistent policy and legislative framework within the country.

The third thing is evidence with respect to cyber crime. Now, if we want to sensitise and prioritise at the legislative level, this is very important. When we start looking at all these cases with respect to electronic evidence for cybercrime, then I hope legislations will uphold much higher authority in the realm of rules.

In terms of institution capacity, we need to take definite steps. The cases are piling up at the Cyber Appellate Tribunal as there is severe shortage of judges. Symantec, along with NASSCOM, is doing capacity building for five curriculums for the National Skill Development which was unveiled last month and has rolled out in different colleges.

For critical information provisions, we have three protected systems in India like the Communication System acquired by the Delhi Police during the Commonwealth Games. The second is Ministry of Shipping and third is Aadhaar CID Act. Apart from these, we do not have protected systems. Unless and until these are protected, the law does not allow higher level of penal provisions. We need to increase our critical information infrastructure, be it the Income Tax database, Voter ID database, RTGS switch, NEFT switch, international gateway of operators and others. Recently, the US has identified 16 sectors which include waterways and dams.

Harmeet Kalra: Given the three pillars that we define problem are people, process and technology. We believe people and process are much bigger problems. Our opinion is that tangibility from technology is far more doable. Pointing out the combat, the firewall market is $200 million and application security market is $6 million. If we pick up any attack on cyber infra only novices attack the actual user. Experts attack application and users are missing the application part on the top of this gigantic wave of digital. As we move towards digital, it is more important to start respecting the fact that it is the applications which the infrastructure is serving. And the focus on application security is right from the building stage of the applications.

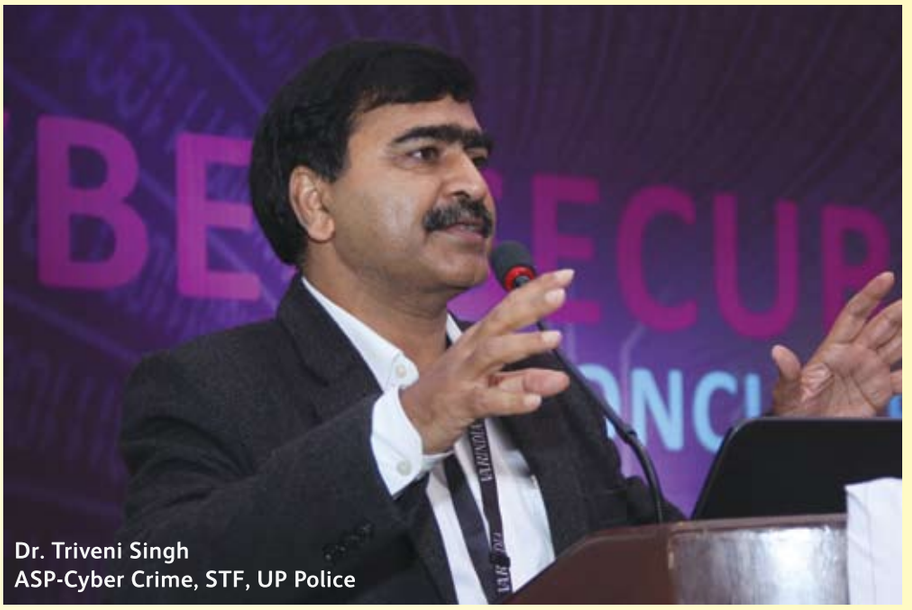
Delhi NCR is the cybercrime hub for India. During the last 16 months, I have arrested 600 boys and girls in the Delhi NCR region, who were involved in cybercrimes. In one instance, through SQL Injection in database, the person was able to recharge Rs.25 lakh.

Cybercriminals are just graduates and through data tempering tool they can bypass the payment gateway. Recently, a computer graduate from Skyline through social trade created a big empire of Rs.3,700 crore, which was cracked. The company had 6.5 lakh users and had around 9 lakh user IDs. The graduate Abhinav Mittal has been arrested and jailed, but the social media campaign is still going on.

We only focus on preventive measures and detective measures but we do not focus on investigation. Investigation requires shared resources both on technical and legal front.

Police is not up to the mark. We are training them and we have also hired the best of consultants. Anybody can spoof your mail ID and mobile number. In cyber black market you can buy anything – be it insurance fraud, debit card cloning and credit card cloning. Each and every crime is a cybercrime nowadays.

Laws are not stringent in terms of cybercrime. For some, it is 7 years; otherwise, it is a non-bailable offence. The whole fraud supply chain is working in Delhi.



Dr. Triveni Singh
ASP-Cyber Crime, STF, UP Police

1. Each and everyone has to be aware.
2. 90 per cent of cases have used social engineering tricks.
3. Massive campaigning against awareness each and every user.
4. Capacity building for police, prosecution and judiciary.
5. Curriculum in university should have best of real experiences of police department and legal fraternity. Cyber forensic is an important aspect of cybercrime.

Amit Malhotra: If you look at the history of leaks, the majority of the leaks happen by trusted source. There is lot of focus on inbound protection. Missing on the 90 per cent data which is outside of the data center. Private banks and government banks are deploying the best of cyber technology.

All of us on the vendor side and also on the enforcement would agree that banks and telecom sector addresses there cyber security requirement. The challenges are coming with respect to information movement. The big boss tells somebody to e-mail top 100 customers. The e-mail comes on the mobile phone and it is not protected. Today, credit cards and banks will have the best of security, but the statement has to be printed and you have to go to the third party and there is an information flowing through a secured firewall. Data center to an outside world and do not know where it is going. And so what we believe in Seclor and that is the stuff we are looking at is instead of data of looking at data centered security we have to look at data- centric security. The data which is moving out in any form – be it a file, a pen drive, through network and peer to peer if you can provide security to that piece of data and security travels with that that potential is the best form. Other which is more critical is maintaining logs and audit trails.

Harold D' Costa: Data Protection law has to be encrypted and domain registration has to be governed by Indian authorities. ■

Pravin Prashant
pravin@varindia.com

Kiren Rijiju Keynote Address Continued

Recognizing the strategic dimensions of cyberspace, the Government created the post of a National Cyber Security Coordinator in 2014. The Cabinet Committee on Security, in its meeting held on 5th October, 2016, approved the creation and administration of research and development fund for cyber security. A high-powered committee has also been created under the chairmanship of the National Security Advisor for setting priority for research and human resource development. To protect the government cyber infrastructure, information security guidelines and cyber security policies have been also issued by the Government. Government agencies and approved agencies are carrying out cyber audit of the government infrastructure. India must develop both offensive and defensive cyber security capabilities that must be robust enough to detect and nullify any cyber warfare against India. Cyber terrorism, attacks and espionage against India is as important as it should be. Today, protecting key economic assets like securing financial backbone and stock exchanges, payment infrastructure and financial switches are the need of the hour. This includes architecting security for new-age banking to make them cyber secure.

With the growth of enterprise mobility, mobile applications and cloud enablement that are driving businesses, techno legal issues have become more prominent. Social networking platforms have further complicated the scenario. There is a need for having public-private partnership in cyber security for protecting the critical online data in creating awareness among public.

There is also a need for establishing India as a global hub of development of cyber security products and promoting indigenization in research and development. For that, a conducive atmosphere has to be created. Developing the human capital remains a priority and the existing gap between the required and available resources has to be made good by the private sector. Higher educational institutions catering specially towards cyber security should be developed, but in the meantime better placement and recruitment practices should be promoted to shore up the manpower.

One of the most urgent needs is to establish an inclusive mechanism to regulate cyberspace. The best way to ensure cyber security is to form an appropriate legal regime for the various types of cyber threats, i.e. cybercrime, cyber terrorism and cyber warfare.

The global cyber security market is expected to reach approximately $190 billion by 2025 from the present $85 billion and will be driven primarily by increasing digitization wave and smartphone penetration. The market is expected to grow at a CAGR of 8.2 per cent from 2015-25. According to Nasscom and DSCI, the Indian IT industry has charted out Vision 2025 to grow the cyber security products and services industry to $35 billion, create one million cyber security jobs and 1,000 cyber security start-ups by 2025.

These are the efforts which will take India into a mode where India will not only be a strong nation but will be a safe nation. We are bound to embark on this journey and the responsibility also lies with state governments. We have been asking the state governments to give a thrust to security.