You & Me

In conversation with the trend setters, the visionaries and the domain experts, who have proved their mettle in the Information Security domain with time. Let us have a concise roundup with our featured personalities, who would present their views over the Information Security trends. This would motivate the readers and enhance their knowledge and vision to take up InfoSec profession and handle challenges in an effective manner.

Honorary Prof. N Balakrishnan
Indian Institute of Science, Bangalore

Prof. Sukumar Nandi
Indian Institute of Technology Guwahati

Prof. V. Kamakoti,
Indian Institute of Technology, Madras

Mr. Mathan Babu Kasilingam
Chief Information Security Officer, NPCI

Hon' Prof. N Balakrishnan
Indian Institute of Science (IISc) Bangalore

The Information Security Education & Awareness (ISEA) programme conceived by the Ministry of Electronics and Information Technology is a very timely, highly impactful and visionary programme. Its impact has touched everyone- Citizen, Government, Corporates and Academia in their daily life. With the exponential growth in the digital transactions there is a need to spread awareness in order to counter, contain and mitigate cybercrime, cyber frauds and attacks on the individual's privacy and the nation's digital and financial assets. Fintech, which is an integral part of common man's life, has become the biggest and easy target for criminals.

With the massive growth in the usage of social networks such as Facebook, Twitter, Whatsapp, etc. it has also become necessary for the users to realise about protecting their identity from being stolen, and also the ability to detect fake and terrorists related news as well as the ability to use these media responsibly. It has also become necessary in today's world to identify the misuse of the social media by others, avoid and shun them if needed.

On the national front, all our critical, financial as well as citizen-related information are available and accessible through the Internet. It is an important role of the Government to protect these information infrastructures against attacks by adversaries who may range from script-kiddies to state actors. Internet has also been off-late used for terror related anti-national activities. Protecting our cyber networks from being used against the nation is also one of the paramount duties of the Government.

ISEA Programme addresses the manpower needs of all of the above issues and brings together all the stake-holders so that the nation's cyber threats can be understood and addressed together. After a tremendous success in the first phase, ISEA continued to expand its outreach to the citizens ranging from school children to housewives to create the awareness and to train them in the safe and efficient usage of the electronic interactions.

In order to address the needs of the industry and the Government, ISEA has stimulated the introduction of courses on Information Security at the BTech, MTech and PhD levels across scores of universities and higher educational institutes in the country. To this end, it created the model syllabi for all such courses and it also conducted several courses from the list of courses that it had prepared. For training the trainees and Government officers, ISEA across its ISRDCs and RCs regularly conducted short-term courses. These had in fact enhanced our capacity as well as understanding and appreciating the cyber security issues.

It had also conceived a very advanced training programme for the Government officers, who would then come back and train more people who would address the important shortfall in manpower requirements. ISEA conducts international conferences which are used as a platform to meet and interact with some of the top international experts. These conferences have also become a virtual ground for interaction amongst ISEA community. Some of the international visitors had also given short-term courses on contemporary topics.

One of the crowning achievements of ISEA is its emphasis on research measured by the number of PhDs produced and the papers published, as well as products developed. ISEA's achievements on these fronts are commendable and have placed firmly the Indian research on the global map.

The way by which ISEA is centrally monitored by the Project Management Unit has brought in a new style of outcome-based monitoring and fostering the projects amongst the S&T community. Overall ISEA Is one of the most successful and relevant programme in today's digital world.

In Conversation with a fabulous professor noteworthy administrator, a technical stalwart and a man with great vision.

Prof. Sukumar Nandi
Indian Institute of Technology (IIT), Guwahati

Cyber criminals are more powerful and cautious but not all critical infrastructures are strong enough to resist a cyber attack. A cyber attack on critical infrastructure could be a preferred mode of attack in a future war. What are the measures taken by government to protect critical infrastructure like telecom ?

In India, Telecom is now a privatized sector with multitudes of operators. BSNL is the only state player in this field. This means that the Indian government has no control what security measures the operators take. All the government can do is release a set of guidelines on the minimum security practices an operator must follow to stay in operation. If an operator fails to meet the guidelines, their license should be withheld and operations ceased. Examples of guidelines are: calls and SMSes originating and terminating in India should never leave Indian borders, call tapping is illegal unless requested for by a warrant, etc. Given the poor enforcement of telecom security in India, I doubt if guidelines exist or existing guidelines are even followed.

Coming to Internet traffic, the Indian Government has installed stateful deep-packet-inspection firewalls at places where undersea fibre cables leave the nation. They are used mostly to block illegal drug sales, block child pornography, prevent piracy of movies and prevent access to government-operated IP ranges from foreign nations. Some of the firewalls even absorb moderate amounts of denial of service attacks. Apart from that, it is difficult to grant government full responsibility. If government agencies are given full control of Internet traffic, the situation may end up like China, where the firewalls end up being used for censorship instead of blocking any real threats. Also granting full control means regular invocation of the Section 69 of the Information Technology Act of 2008, which will force private key disclosure or forceful decryption of all secure communications by law, thus making the premise of end-to-end secrecy null and void. This will have an unintended side effect. Enemies of the

state will be able to gather data about Indian citizens by deploying agents in the Indian government and telecom operators.

Considering that Chinese companies like Huawei and ZTE manage most telecom operations in India, forceful decryption of encrypted traffic only means most of our trade secrets will be siphoned to China. The proper alternative to this is to allow the government to lay down a list of security guidelines for ISPs to follow if they have to operate in India, and leave the implementation to ISPs and end-users in a privacy respecting manner. If someone does not comply to the guidelines, legal action can be pursued. This ensures that government focuses on enforcement, while the end-users and ISPs can protect themselves with their own security measures and encryption tools. Privacy and freedom of choice are complementary with security, not exclusive to one another.

The IT threat landscape is becoming more complex with the emergence of sophisticated threat variants every day. Cyber terrorists are now rapidly shifting their focus towards critical infrastructure and strategic industries to bring down the nations by causing deadly damage. Cyber weapons are being used to bring the critical industries to a standstill. Why India needs a robust mechanism to secure critical Infrastructure?

I have only two things to say:

a. *Do not put critical infrastructures/ devices (like factory equipment and nuclear power plants) on the public Internet. If you require remote access, use a VPN or a secure authentication layer to access the internal network. If you have enough manpower to handle equipment, completely air-gap the internal network from the external one and request an employee to copy required data back and forth using removable storage. This is enough to avoid most threats.*
b. *You have already answered the question you asked.*

Critical infrastructure being a soft target of cyber crime syndicates could lead to disastrous consequences if the systems are prone to outsiders as well as insider threats. Is India prepared for Industrial security ?

Going by the current trends of cyber security in Indian companies. हम सब के सब मरेंग।

Public Wi-Fi is a hotspot for cybercriminals. What are steps taken by governments to reduce the cyber attacks that happen through public Wi-Fi ?

See second part of answer to Question 1. Government should mandate and enforce, not operate/implement.

Cyber criminals can steal personal information, data from private or government organisations, disrupt services, cripple the financial system and trigger national security. Cyber security is one of the important national security challenges that countries face all over the world. With all these has government formed any conceptual framework for cyber security awareness and education ?

Yes, MeitY is running cyber security awareness campaigns and workshops across the nation as part of Information Security Edujon and Awareness (ISEA) Project.

According to Google Trends, Ransomware is a very popular search word these days. What are your thoughts about it? What changes or trends do you expect to see in cyber security in the next 10 years?

According to me, ransomware is an epitome of how creative humans can become at extorting money. For bad actors, ransomware is a sure-shot way of earning fast bucks without the headache of taking over a corporate network and demanding money to release it or the risk involved in selling private data to competitors. All a ransomware developer needs to do is let it infect PCs, and wait for the owners of the PCs to pay the ransom amount in digital or plastic currency to fetch the decryption key needed to restore the encrypted files to original form. All of this happens in an automated manner, and requires no manual effort or communication to the victim by the bad actor.

Ransomware uses modern public-key cryptography, and there is little chance of getting your files back if you do not pay the ransom amount. Some popular ransomware have had bugs and kill switches revealed by security researchers, who have contributed successfully in stopping the spread of the malware. But a well-written ransomware without any backdoor or kill-switch to turn off is inescapable once your computer is infected. So, regular full backups are the best solution to save yourself from a ransomware attack. Also, try to avoid unknown and unverified apps on your computer.

Another important thing to note is that ransomware is gaining traction rapidly because of Windows' flawed security model. The lack of proper user access and permission control to sensitive files is a huge contributor to this problem. You are simply one 'Allow' button click away from losing your files and destroying your Windows system. If possible, switch to a better OS, like GNU/Linux or macOS.

Evolution of cyber security is something that cannot be predicted well in advance. We find new threats every day and fix current ones every day. It is a cat and mouse game between system builders and system crackers, which is not going to end anytime soon.

With the increasing focus of the Government on digitalization of the country, most of the transactions have acquired a digital form. It is necessary to create awareness among people regarding the importance of cyber security. How awareness help as a first line of defense to tackle cyber security threats ?

This is very obvious. If you know how a system works, you can deal with its problems better than someone without any clue. Is there anything to explain here?

What is your take on information security of your organization? What technology development do you find most perplexing from a security point of view? Based on changing threats and emerging technologies, how do you see your organizations IT security policies and technical approaches changing during the next 12 to 18 months?

IT security of most Indian organizations is sub-par. Most non-financial and government organizations do not follow even the minimum in security practices. Going in this direction, every development is perplexing to deal with, considering the lack of talented personnel, unwillingness of employees to follow security practices, political interference to change and bureaucratic inefficiency. जो दस साल में नहीं हुआ, वोह क्या घंटा 18 महीने में होगा।

Biometrics is like passwords you leave everywhere. What is the role of biometrics in cyber security and will biometrics be the key to attain a cyber secure world ?

Biometrics are a convenient way to authenticate a user but is not secure. Biometrics are prone to misuse because they cannot be changed easily. For example, a robber may forcibly show your face at gunpoint to a Face ID operated ATM to withdraw cash. They can also unlock your phone simply by pointing the phone at your face. Also, it has become incredibly easily to bypass fingerprint verification. One can make a clone of your fingerprint in high grade silicone wrapper, wrap it over their finger and place it on the fingerprint scanner. To the system, it is like you have authenticated

with your fingerprint. You cannot prevent similar actions in the future, because you cannot change your biometrics at your will or convenience.

Another problem with biometrics is that they can change when you least expect it. For example, if you injure your fingers, your fingerprint may change to some extent when it heals. Your face can change after reconstructive surgery following an accident. Your iris can be damaged due to injury in your eye. All of this can make biometrics extremely unreliable in the long run.

Someone proposed an alternative to biometrics, i.e., DNA based authentication using tears, sweat or spit, which is a great option, considering DNA changes very minutely over the entire lifetime of a person. But it again runs the risk of misuse: someone can collect your body fluids, store them and later authenticate as you.

In my opinion, neither biometrics nor DNA alone is the key to a secure future. Sure, they are a great convenience in low to medium security cases. But if high security is needed, I would suggest a 3-factor authentication scheme, based on who you are, what you have and what you know. So, the first factor will be your biometrics, the second will be a code generated from hardware device given to you and the third will be your password or a phrase only known to you. A bad actor is unlikely to possess all three at the same time, thus thwarting most impersonation attempts. If this scheme becomes a standard, it will be near impossible for people who have never met you to steal your identity.

IIT Madras has identified "Secure Systems Engineering" as the thematic area for research in the Information Security area under the ISEA Phase-2 project. Building a trusted system involves establishing a Root of Trust and a chain of trust. The "Root of Trust" need to be established at the Hardware which in turn, shall certify a microkernel for functionality. The microkernel in turn shall certify the kernel, file systems and so on thus establishing a Chain of trust. The research and development involves architecting this Secure stack, right from Hardware Microarchitecture to Secure operating systems. As a part of this effort, IIT Madras has initiated research on basic cryptography, developing primitives for low-power security algorithms, block-chain based approaches to ensure information integrity, and secure and attack-resilient network architectures. On the education front, over the last five years, IIT Madras has offered five courses (one per year) on the different layers of secure systems engineering under the NPTEL-MOOC platform. Several thousands of people had enrolled for these courses. The lectures are available free for all interested. In addition, IIT Madras is offering online MTech in Information Security for industry professionals.

Prof. V Kamakoti
Associate Dean,
Industrial Consultancy &
Sponsored Research (IC&SR)
Indian Institute of Technology Madras

In Conversation with technogient in IT / ICT technologies for financial institutions

Post demonetization Digital payments have increased by many folds. The government is taking a lot of efforts towards creating a cashless society and has launched many payment methods like Aadhaar based mobile payments, BHIM (Bharat Interface for Money) which works with fingerprint authentication. In view of various cyber attacks reported on these methods, how do you combat to such attacks?

Perpetrators always try to identify issues NO MATTER how secured an application is built easily by largely leveraging issues found in underlying Operating Systems like Android, iOS etc.. It is important to build applications that are able to Secure itself not just in Code but as well in Run time. To this effect, NPCI constantly publishes guidelines around Secure Practices to be followed by Applications that leverage any of NPCI services and we too constantly improve our own applications like BHIM.

Digital payment technologies are slowly becoming a close substitute for cash and have led to an increase in the role of non-banks and non-cash payments in the payment process. What are the implications of these developments in India? What are the different issues and challenges in current payment methods? And what are the measures taken up to overcome the challenges ?

The primary issue is to identify the digital user and establish the trust. Earlier conventional methods of Banking had various methods to verify the source (physically) before any transactions are made and the number of NON-REPUDIATION instances were minimal. With evolving Digital Channels in Banking, it is important to establish such NON-REPUDIATORY TRUST with the Digital Identity of the User, which most often is USER NAME & PASSWORD or MOBILE NUMBER & Password combination.

Mr. Mathan Babu Kasilingam
Chief Information Security Officer, NPCI

To make any Financial transactions secured, it is critical to have 2 factors and preferably SOMETHING YOU HAVE or SOMETHING YOU ARE & club it with SOMETHING WITH YOU KNOW.

The above makes Digital Payments tougher to break. But the challenge here again is that determined fraudsters most often leverage conventional Social Engineering practices to obtain all of the above parameters from the customer making it difficult to stop such attempts.

Creation of Digital Awareness to this effect are being undertaken by various players including Government & NPCI to create User Awareness which is critical in tackling such crime.

National Payments Corporation of India (NPCI) being a prime organization for all retail payments system in India. What are your awareness initiatives to educate about different types of financial frauds and how to avoid these frauds while using various digital payment systems?

Awareness initiatives are both internal and external facing and efforts are made through various marketing campaigns and advertisement / announcements made in News paper publications, joint co-branding with multiple financial players etc in their messaging to users, leveraging Short Messaging Services that are sent during any financial transaction etc are few to name.

As chief information security officer (CISO), you are responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. What would be your suggestion for public to take necessary security tips with respect to your products like UPI, BHIM etc.

The critical quotient in the Digital world is

1. *"TRUST BUT VERIFY" – Trust the applications that are only hosted in the NATIVE PHONE's APP STORE but choose to VERIFY the App's and its permission levels to other critical functions in the phone*
2. *Phone and the Digital identity (User name & Password or Email address / Phone Number / SIM Card & Password / OTP) are critical factors to protect and never reveal any of these combination to any person who is asking you for all of these information in any combination.*

PROTECT YOUR PASSWORD

Password is a key or a Secret word or a string of characters which is used to protect your assets or information from others in the cyber world. It is used for authentication, to prove our identity or to gain access to our own resources. It should be kept secret to prevent access by unauthorized users.

In social networking sites like Facebook, Orkut, and LinkedIn each of which is studded with answers to commonly used security questions such as favourite place, school, college, etc..

You are responsible for safeguarding your ID and password

Things to be remembered while creating Strong Passwords

- Use at least 8 characters or more to create a password. The more number of characters we use, the more secure is our password.
- Use various combinations of characters while creating a password. For example, create a password consisting of a combination of lowercase,
- uppercase, numbers and special characters etc..
- Avoid using the words from dictionary. They can be cracked easily.
- Create a password such that it can be remembered. This avoids the need to write passwords somewhere, which is not advisable.
- A password must be difficult to guess.
- Change the password frequently at least 2 weeks once

Guidelines for maintaining a good password

- Change the password once in two weeks or when you suspect someone knows the password.
- Do not use a password that was used earlier.
- Be careful while entering a password when someone is sitting beside you.
- Store the passwords on computer with the help of an encryption utility.
- Do not use the name of things located around you as passwords for your account.

Hard to remember PASSWORD ?

Switch to a PASSPHRASE

My passphrase Never judge a book by its cover

My password nJ@66!C

never Judge @ 6ook 6y !ts Cover

What will your passphrase be ?

For more details / queries on
Cyber Security visit or call us to our Toll free number

Ministry of Electronics & Information Technology, Government of India

www.InfoSecawareness.in 1800 425 6235

For Virus Alerts,Incident & Vulnerability Reporting
CERT-In Handling Computer Security Incidents
http://cert-in.org.in/

www.cyberswachhtakendra.gov.in