National Centre of Excellence
for Cybersecurity Technology
Development & Entrepreneurship

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Ministry of Electronics & Information Technology
Government of India
सत्यमेव जयते

PRESENTS AT

AISS 2020
NASSCOM-DSCI
ANNUAL INFORMATION SECURITY SUMMIT

SERI
Security Education, Research, & Innovation Conference
Promoting Cybersecurity Education, Research and Innovation

SERI CONFERENCE

POST EVENT REPORT

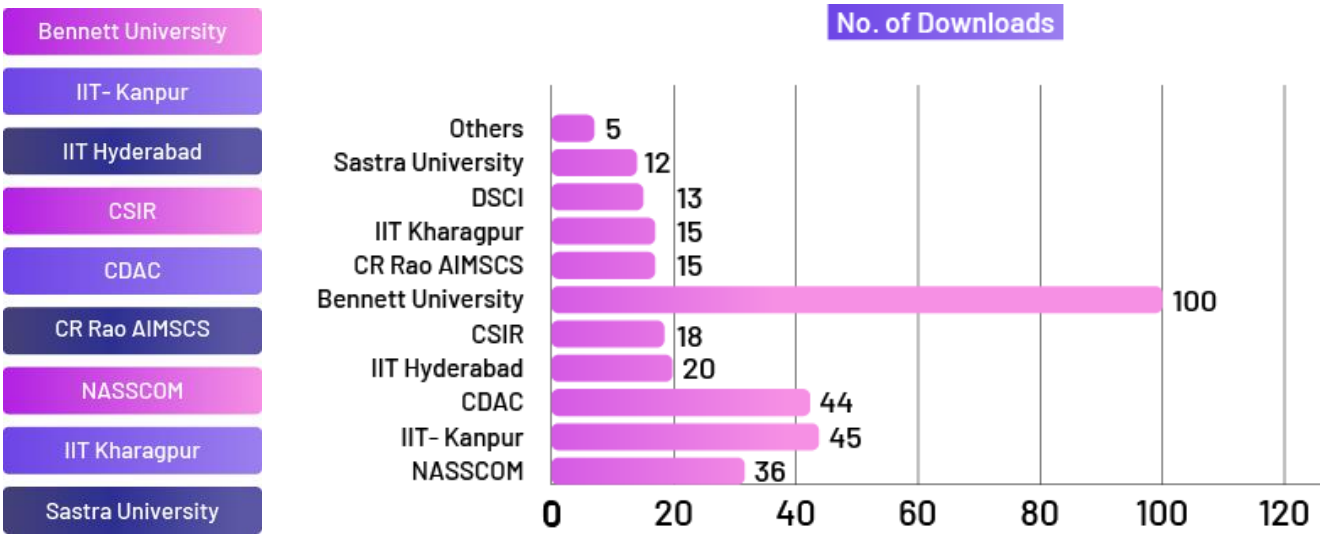
14th DEC 2020 | 11:30AM to 8:00 PM

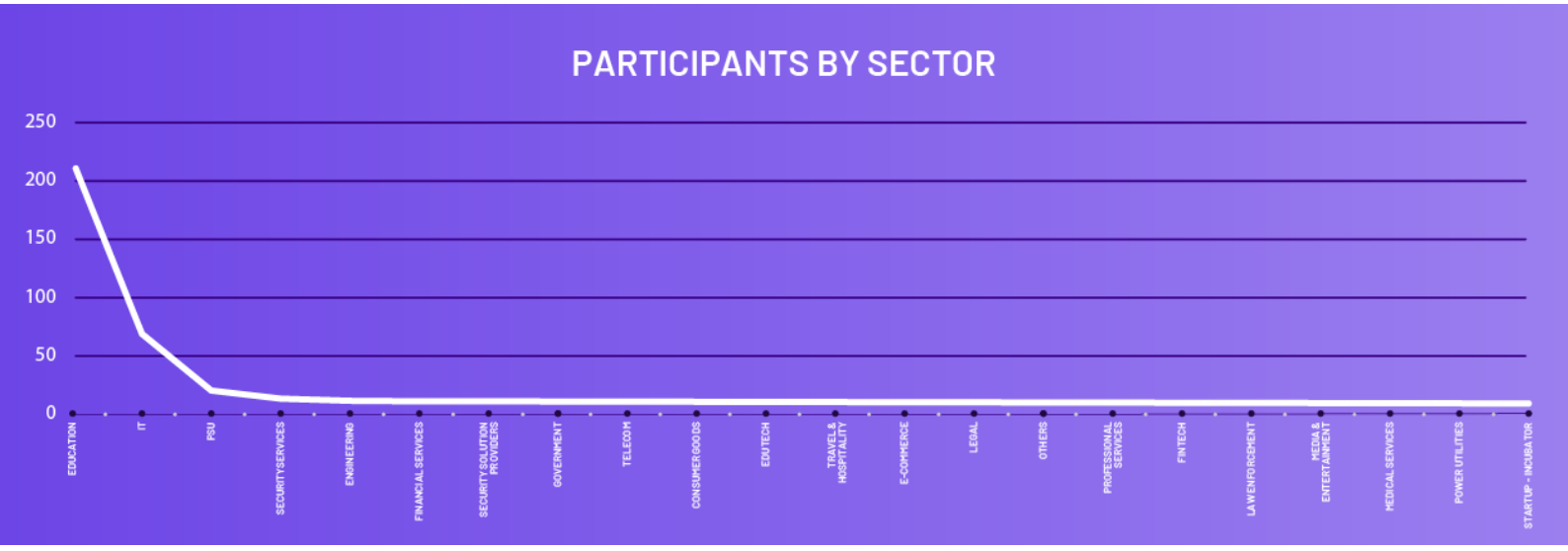
CONTENTS

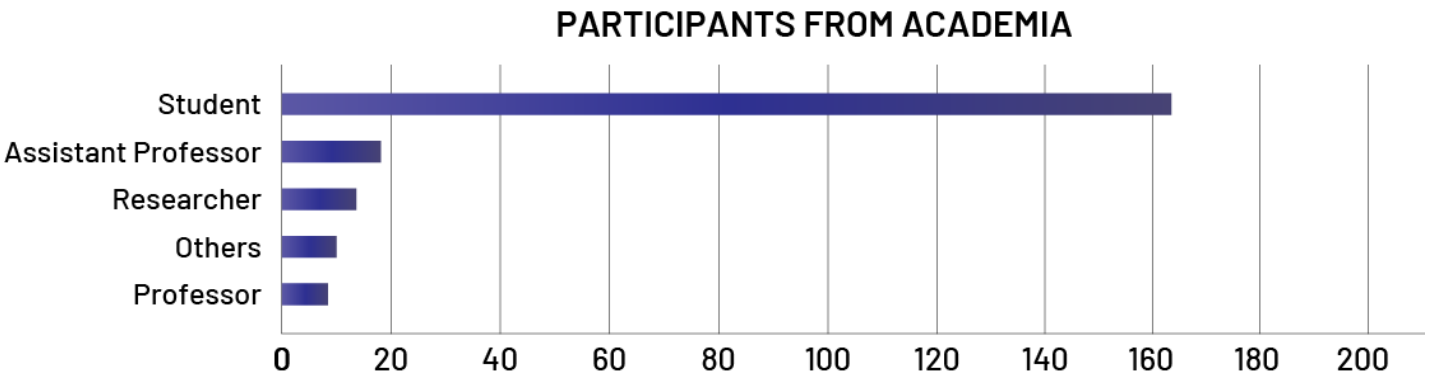
Event statistics:

Participants	Research Paper Presented	Speakers	Networking Opportunities Facilitated
385	11	37	235

Exhibit visits:






PARTICIPANTS FROM ACADEMIA
Student
Assistant Professor
Researcher
Others
Professor
0
20
40
60
80
100
120
140
160
180
200

Cyber East: University Education & Research ... Australia, Singapore, and India

Plenary

- **Prof. Maninder Agarwal** - IIT Kanpur
- **Prof. Greg Austin** -School of Engineering and Information Technology UNSW Canberra
- **Mr. Ch A Murthy** – Associate Director, C-DAC
- **Mr. Ajay Kumar** - Asia Pacific Cyber Security Business Leader, DSCI Singapore Chapter Anchor

Moderator: Mr. Vinayak Godse - VP DSCI

Session summary:

As the topic suggests, the discussion was around various initiatives and experiences for university education and research in Australia, Singapore, and India. The panel highlighted few marquee initiatives in each country and shared key insights on how Universities can lead the agenda around innovation in cybersecurity and privacy domains.

Organizations focus on people, process, and technology as core areas from a cybersecurity perspective. The people hold the key as they are essentially responsible for executing technology strategies and design, development, implementation, and governance. Thus, the need to hone cybersecurity skills during the undergraduate level and ensure cybersecurity concepts are introduced at the school level is especially important.

Singapore has developed a detailed master plan for its cybersecurity and is also working towards eliminating the gap between the supply and demand of cybersecurity professionals. Both Singapore and Australia have been able to create platforms for collaboration between academia and industry. India, too, has several initiatives with institutions of national repute. For example, the C3I at IITK Center was established in 2016 in the Computer Science and Engineering of IIT Kanpur for research, education, training, and awareness campaign on cybersecurity of critical infrastructures in India. Information Security Education & Awareness (ISEA)- a MeitY funded project has been underway in India to build information security capacity, address human resource requirements in the country, and create mass information security awareness. Given the three nations' experience in tackling cybersecurity education and research challenges, it is desirable to develop a regional knowledge and talent hub between the three countries. Such a hub can provide impetus to collaboration activities in curriculum and courseware development and create avenues for student exchange programs. All countries are currently grappling with addressing the shortage of skilled cybersecurity workforce and have developed strategies to address the need only in their

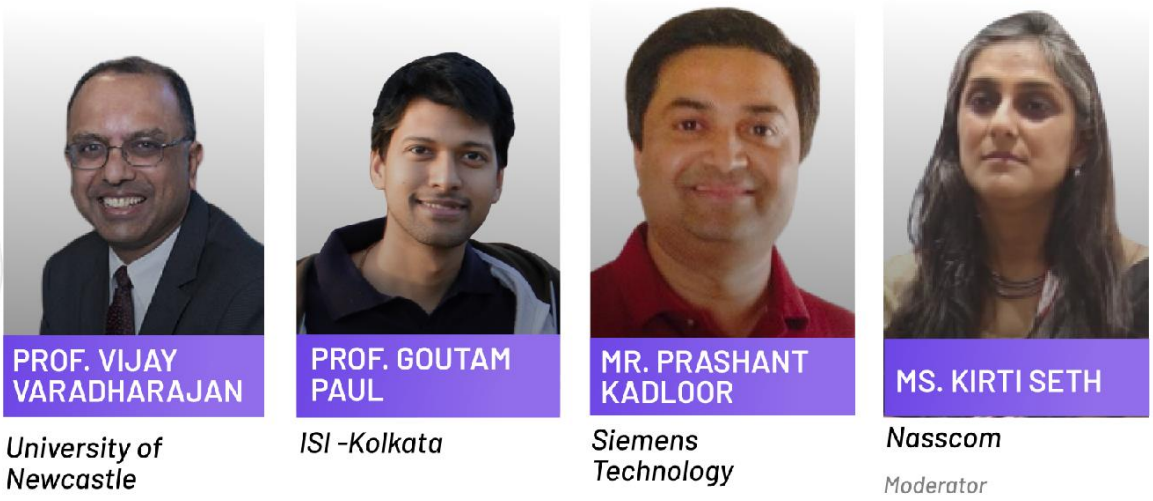
own countries. Such a centre can also be set as a base for exporting cyber skills to strengthen the ASEAN region and eventually cater to global requirements.

Attracting Young Minds...For the Depth of Security & Responsibility of Privacy

Track Session:

- **Dr. Vijay Vardharajan** - Professor, University of Newcastle
- **Prof. Goutam Paul –** ISI Kolkata
- **Mr. Prashant Kadloor** – Head of research group cybersecurity Siemens Technology

Moderator: Ms. Kirti Seth FutureSkills Lead, NASSCOM



Session summary:

The panel deliberated on possible strategies to attract/ motivate young people to pick cybersecurity and privacy as a career/research option.

Cybersecurity is much more than solutions and technology and involves aspects from other disciplines such as legal, social sciences, and international relations. Cybersecurity can assume many forms, right from rudimentary examples like non-repudiation of information to the authenticity of information exchanged to the more complex ones such as the global supply chain-related cybersecurity issues. While cybersecurity is linked with everything around us, and people of all ages need to be aware, students are apprehensive of picking a cybersecurity career. It is widely believed that coding and programming skills are essential for a career in cybersecurity; however, students from various streams can build their career in this field. For example, if someone is good at mathematics, they can hope to develop cryptographic algorithms. Likewise, students from art or design can do well in UI/UX design in the cybersecurity solutions space. While technologies such as Machine Learning (ML) and Artificial Intelligence (AI) have caught students' fancy, cybersecurity is yet to emerge as a preferred career option. The intersection of Machine Learning (ML) and cybersecurity is the need of the hour as we look at the increase in smart devices' adoption. As autonomous devices make decisions, there is a need to ensure that the decisions conform to design norms and established rules. These scenarios will emerge in the coming future, and the current generation of students shall need to be ready to address such challenges. Similarly, cybersecurity and Artificial Intelligence (AI) shall need to intersect to make algorithms

more secure and dependable. Smart infrastructure and Information Technology/Operational Technology (IT/OT) convergence is another area where cybersecurity professionals' needs shall grow.

While a tremendous amount of opportunity exists, and several initiatives are underway in the country to demystify students' cybersecurity career options, a lot more needs to be done. Focussed campaigns on coaching students about the need for cybersecurity as a career option or as an integral part of any career in the future are the need of the hour. Young minds need to be tuned and oriented towards problem-solving in the digital world as the world becomes a system of systems, and interconnectedness becomes ubiquitous. For example, IISC has been organizing summer schools and summer internships for cryptography and organizing talks from other Industry stalwarts on developing cybersecurity skills. Various methods, such as simulation-based training courses, e-learning platforms, hackathons, and gamification techniques, need to be leveraged to keep students engaged.

Automated Reasoning ...How would it's transforming security decision making

Track Session:

- **Mr. Vinayak Godse,** VP DSCI
- **Prof Ashutosh Gupta,** IIT Bombay
- **Prof. Dhiman Saha,** IIT Bhilai

Moderator: Prof. Debayan Gupta, Ashoka University

Session summary:

The session revolved around understanding how automated reasoning capability shapes up to solve many use cases for security decision-making and around factors that influence automated reasoning-based systems' accuracy. The panel members also discussed how automated reasoning could help organizations meet customers' and regulators' mandatory requirements.

Nation-state actors are using complex techniques such as acoustic cryptanalysis to break encryption techniques. It is challenging to come up with models that could detect and prevent such attacks. Detection can be made better with machine assistance for a few categories of attack, such as the side-channel attack (vulnerabilities exploited in the implementation part). An

example was the Triton malware attack on an Industrial automation system in 2017. The system had layered security and was in an isolated private network, disconnected from the internet through firewalls and access controls. Though, in this case, a vulnerability did exist due to a misconfigured firewall, automated systems and models could have helped avoid such a scenario. Automated reasoning models revolve around analysis and discover all the possible errors/ misconfigurations against established policies or frameworks. Such models can also help policies evolve as the operating cycle of security progresses, and deterministic policies for security scenarios are devised to withstand the scale and complexity of attacks introduced in any environment.

With the need to comply with cybersecurity and privacy regulations, frameworks, and practices growing with requirements placed by an ecosystem of regulators, insurance companies, industry bodies, and other stakeholders, scoring systems at procedural or outcome levels becomes more difficult. Automated reasoning-based systems can be used in such scenarios to judge how to secure systems and help decide cyber insurance premiums through quantitative scoring of networks. A few technology-focused unicorns are taking a keen interest in data science and computer science fields in India. In the last few months, a lot of investment has been made in cloud technology in India. This has also led to corresponding investment in security technologies. The banking sector focuses efforts on cyber defense centres (CDC), which develop orchestration for security and can benefit immensely by leveraging automated reasoning capability. With the Data Privacy Bill's developments, larger conventional companies may also start looking at automated reasoning to solve their compliance needs. The MEITY funded and DSCI led National CoE has also been encouraging research activity in this space and is trying to play a role in identifying researchers in this domain. R&D centres such as CDAC have already been working on other cybersecurity-related areas for a long time. The National CoE is trying to facilitate access to industry data for such institutions to further aid development.

Inaugural Session:

- **Mr. Amit Aggarwal,** CEO, IT-ITES Skill Council of India, NASSCOM
- **Ms. Rama Vedashree**- CEO, Data Security Council of India

CEO, Data Security Council of India

CEO, Future skills

"Think Digital, Think India" has been the charter of NASSCOM. Similarly, DSCI has been working with the charter of "Think Security, Think India." For India to become a global hub in cybersecurity, a lot more needs to be done. We need to foster collaboration between academic institutions, industry, and government, especially institutions and labs in critical infrastructure, to realize this charter and make India a global cybersecurity leader. The Ministry of Electronics and Information Technology (MeitY) and DSCI have conceptualized the National Centre of Excellence (National CoE) to enable an ecosystem where cutting edge and technology-driven research can be undertaken.

This is to help build the foundation for an environment where products made in India can cater to the needs of both the domestic and the international market.

Digitization paradigms and the adoption of emerging technology has brought cybersecurity to the forefront, at times as an enabler and at times as a showstopper. Thus, technology development and the discovery of new use cases are of prime importance to solve any bottlenecks. All stakeholders need to work collaboratively to evolve use cases and undertake cutting-edge research to innovate and build products. With government research labs' support, the National CoE already enables several deep-dive technology collaborations in hardware security, IoT, and cryptography. The National COE is also a platform for young start-ups to emerge from. Its initiatives are organized to facilitate the commercialization of products and encourage the growth of domestic IP. The National CoE also enables students and researchers to participate in workshops organized on cryptography, IoT and hardware security, etc. Worldwide, academic institutions lead the way for R&D. To commercialize products, subject matter experts, government research labs, and the user industry need to partner together.

The impact of COVID-19 has been to accelerate the adoption of technology across various sectors. It is often stated that ten years of growth was witnessed in 4-5 months after the pandemic outbreak. NASSCOM and the industry are geared to appreciate the importance of cybersecurity amid such a surge in technology adoption. Therefore, it is imperative to consider a few essential differentiators which will help guide the industry as they navigate the new normal. The first is trust - the enterprise can now differentiate itself by building healthy security practices. The second important factor is the ability to identify opportunities with a strong tailwind. There has been a lot of effort put into cybersecurity research, and we have sufficient momentum with several on-going initiatives. We need to accelerate the same to accomplish our digital dream. Next, India has a huge opportunity to emerge as a talent hug for cybersecurity talent. The country currently has around 1.8 million professionals in the new and emerging technology space. With cybersecurity, we can take a competitive advantage over other countries, thereby realizing our dream of being the preferred destination for cybersecurity solutions and services.

Special Address

Mr. Arvind Kumar- Scientist G & Group Coordinator MEITY, New Delhi

Digital India has cybersecurity as an inherent strength, as India continues to leverage its position as a global hub for IT R&D and services. The Digital India program's strategy was to promote productization, commercialization and increased security R&D in the country. DSCI and MEITY have combined their efforts to look at emerging technology in cryptography, cryptology, hardware security, and AI/ML application in cyber defense platforms to share and promote collaborations in the cyber landscape. One such project called the cryptographic module evaluation program by IISC and C-DAC uses NIST standards to integrate with national digital platforms. Low power and low resource-intensive algorithms in IoT, 4G, 5G wireless networks, quantum cryptography, and cloud security are key focus areas. Rich innovation ecosystems for tech. Commercialization and product entrepreneurship are required to make India a global powerhouse in cybersecurity.

Keynote

Industry Intervention: Cybersecurity Skill Building... Connecting Dots, Mobilizing Efforts, and Deploying Intelligence

- **Mr. Vinayak Godse**, Vice President, DSCI
- **Ms. Priya Madhavan**, Consultant - NASSCOM FutureSkills

NASSCOM
Moderator

DSCI

Security is the next big thing. One trillion dollars is expected to be spent on cybersecurity by 2025. About 4.1 million professionals are needed for cybersecurity-related jobs globally, out of which around 2.6 million are concentrated in the Asia Pacific (APAC) region. NASSCOM and DSCI have a slew of initiatives to support the Indian cybersecurity Industry's growth serving the domestic and international market and strengthening the domestic ecosystem. Several global players have established R&D facilities in India. For example, large technology organizations such as Juniper, Cisco, etc., as well as technology giants such as Google and Microsoft, continue increasing the headcount of their cybersecurity workforce in the country. On the demand side, such companies are looking for skilled cybersecurity professionals. On the supply side, they help with the upskilling of existing IT professionals and offer avenues to develop cybersecurity professionals. We are also looking at academic institutions to evolve a sufficient range of programs to cater to the increase in demand. Security OEM manufacturers such as Cisco and Palo Alto have also created cybersecurity skill and certification programs to aid skilling efforts. On similar lines, ISACA and other recognized bodies in the certification space contribute to cybersecurity skill-building.

The IT industry is a key consumer of cybersecurity skills. Technology such as AI, ML, and NLP is being used extensively, pushing the demand further for Computer science professionals. There remains a perception gap with respect to the uptake of cybersecurity courses in this hotly contested technology skills space. Specialized cybersecurity degrees are coming up in many universities. DSCI has published a database/dictionary of almost 140 cybersecurity roles mapped to a security analyst role. Such efforts are being made to demystify the needs of various cybersecurity roles, thereby helping universities develop specific modules/ programs to cover for the same. DSCI, in conjunction with NASSCOM, is further building models around skill assessments to aid skill-building. Along similar lines, DSCI has been leveraging its National Centre of Excellence to focus on the national ecosystem requirements for sustained R&D activity in cybersecurity. DSCI is also building an academic network to engage youth within IITs and is developing use cases for AI/ML. Research data set, the repository for cybersecurity R&D. DSCI, is also working on setting up an ecosystem of labs to create visibility for future technologies. A mapping of the research areas currently underway and a list of professors involved are also being developed. Cybersecurity is a crucial area for the start-up ecosystem in the country. DSCI has been putting in efforts to connect all stakeholders in this ecosystem in a meaningful and constructive manner, thereby fulfilling the charter laid down by the country's National Security Policy.

What Industry Expects? ...Roles in Security Services, Consulting Research, Product Security, & Technology Development

Track Session

- **Ms. Shailaja Vadlamudi** – Director & Application Security Lead for SAP Labs
- **Mr. Vittal Raj** – Founding Partner Kumar and Raj, Chartered Accountants
- **Mr. Ashish Khushu** – Chief Technology Officer L&T Technology Services Limited

Moderator: Ms. Priya Madhavan – Consultant, FutureSkills, NASSCOM

The requirement of talent and skill across all sectors is diverse. The panel deliberated on decoding how these requirements are being created and recommendations around strategic interventions at a national level to cater to all sectors' future needs.

The discussion started with various digital transformation initiatives across industries, from process-based engineering organizations to software development and manufacturing. Though the industry has been at the forefront in adopting technology such as robotics, automation, embedded software, and analytics, the need for cybersecurity is being realized now since everything is directly being connected to the internet. Communication or data exchange between different information systems gives rise to a sophisticated network with an elevated risk landscape. Security in the present age is a much more significant concern for the industry than a few years back when endpoint protection and network security with Intrusion detection controls were considered sufficient. Today, it is about establishing the policies and technology that range from governance to operations and ensuring people at all levels are well-versed with requirements to make the organization cyber secure. Cybersecurity encompasses all roles in an organization; from CISO to an entry-level engineer, everyone needs to be security literate. During a product or solution building cycle or software development, the perceived threat level has become much more elevated, to the extent that security is intertwined with technology and cannot be treated as an external attribute. Embedding security as part of a cloud, IoT, AR/VR, and DevOps processes right from conception to rollout are of strategic significance. There is already a demand for architects and design fail-safe systems and devise security posture management strategies that ensure resilience by design. Platforms of trust are shakier than ever, especially in the BFSI sector, with a growing number of fintech start-ups. Banks have also evolved from seeing cybersecurity as a retrofit to incorporating security right into their SDLC. Professionals familiar with security practices, in conjunction with business processes of life-critical domains like healthcare, autonomous driving systems will soon be the most in-demand.

Security Research Bottleneck ... Lab, Program Set-up, Problem Statements, Industry Connects, & Data Sets

Track Session

- **Dr. Sumanta Sarkar** – Research Scientist at TCS Innovation Labs
- **Prof. Charru Malhotra** – Associate Professor (e-Governance & ICT) at IIPA
- **Prof. Somitra Sanadhya** – Associate Professor, CSE, IIT Jodhpur

Moderator: Mr. Vinayak Godse – VP, DSCI

TCS Innovation Labs

IIPA

IIT-Jodhpur

DSCI

Moderator

The panel deliberated on the overall outlook around the security research arena. Further, it strengthened it by coordinating efforts needed to bring together necessary infrastructure and enablers to drive research and innovation, supported by forging partnerships between academia and industry.

Cybersecurity has an important role in securing a nation's strategic interests and has emerged as the fifth domain of national security. Commercial support for cybersecurity is constantly increasing, with more than one trillion investment expected in the next three years. India's challenge is that the industry has not taken an active role in supporting academia. Research is not rising exponentially in line with the needs and requirements of our country. The supply of people willing and capable of working on cybersecurity research areas is less due to the lack of regulatory sandboxes and testbeds to experiment and a lack of infrastructure to practice in an isolated manner without cascading the impact on the rest of the network. A few pockets of innovation have emerged, with the academic ecosystem in India showing progress. Institutes such as ISI Kolkata is leading research in cryptography. IIT Kharagpur is leading research in hardware security, and IISC and IIT Madras are conducting theoretical and applied research. Still, research spending as a percentage of GDP is lower in India than in other economies and is further lower for the cybersecurity domain. Many use cases can be solved with AI/ML but are often hindered due to a lack of datasets. The lack of a vibrant feedback loop between data providers, research entities, and practitioners seem to be the core problem. Initiatives by MEITY such as Cyber Surakshit Bharat to train CISOs and personnel from the government and tri-services to improve their organizations' security posture needs to be ramped up. Such training shall also create avenues of collaboration between institutions, as more organizations realize the benefits of such association in the long term. Organizations such as CERT-in, DSCI, and statutory bodies that deal with crisis management and incident analysis should further explore mechanisms to share available data with universities. The industry should realize the importance of its role in making data available for research

purposes. Setting up labs and short-term certification, diploma, specialization programs would solve the shortage of trainers.

Another major problem statement is improving the visibility of research and mobilizing interest in the security area. Cybersecurity does not have the same hype as deep learning despite the same market size. The industry and students should lead this hype cycle must be incentivized by the industry demand, so it is easy for academia to attract students and train them. The convergence of research agencies like CERT-in, DST, NCIIPC to create a holistic digital platform for advisory, action, alerts like NCSC(UK), and security scholarship programs like in the US could remove some of these research bottlenecks. Efforts from the private sector, such as the TCS fellowship and other corporate, academic programs for higher-level researchers like Ph.D. aspirants, are also worth replicating for various country professionals.

Stronger Security, Resiliency & Privacy...Data, Speed, Volume, Diversity, & Complexity

Track Session

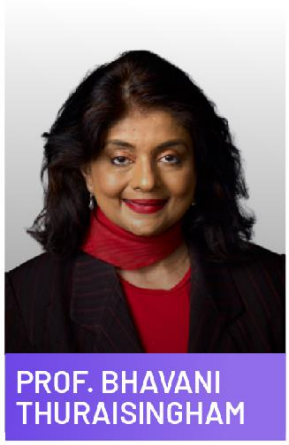
- **Prof. Bimal Roy** – Head of R C Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata.
- **Prof. Huzur Saran** – Professor, Dept of Computer Science and Engineering, IIT Delhi
- **Prof. Sadie Creese** – Professor of Cybersecurity, Dept. Of Computer Science, University of Oxford, UK

Moderator: Prof. Bhavani Thuraisingham – Chair Professor Department of Computer Science, University of Texas at Dallas

Indian Statistical Institute -Kolkata

IIT Delhi

University of Oxford



University of Texas

Moderator

This session was organized to learn about making security, privacy, and resilience-focused decisions to accompany technology adoption and digital transformation. Considering that cyber threats are more sophisticated than ever, and attackers are persistent in their pursuit to penetrate an organization's defenses, dynamic and real-time visibility about the organization's security posture has emerged as the need of the hour.

The discussion initially touched upon the differences between security and privacy by highlighting key attributes. For example, it was stated how security deals with maintaining the transaction's

integrity. At the same time, privacy involves ensuring the identities of parties involved in the transaction are not disclosed without their consent. Such fundamental elements are often overlooked during both the development and the implementation of technology. As a case, the panel discussed the challenges with IoT networks, which involve a massive amount of transaction between the edge device and the central unit; however, due to lack of computational power on the endpoint device, it becomes difficult to even consider fundamental elements of security and privacy from being implemented. The discussion further progressed into ramifications of any attack and lack of tools to model the systemic and aggregated risk associated with regulatory fines, breaches, and rebuilding reputation. With borderless organizations becoming a norm, all organizations need to prepare their insider threat systems and concentrate their anomaly detection efforts. With deep learning in attackers' hands, AI would prove the cyber kill chain framework more potent, especially in reconnaissance and delivering payload stages. With wireless networks becoming more pervasive and fluid boundaries comprising various endpoints, security for cloud and telecom providers will only increase. The trade-off and compromises in privacy, security, and resiliency will still exist in the future; however, this should be decided on a case-to-case basis, and models should evolve from real-time datasets' feedback.

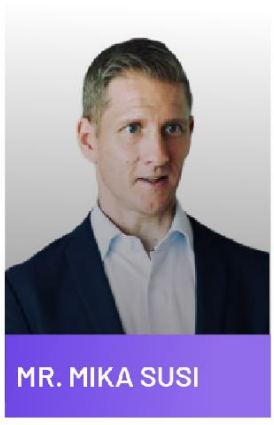
Security & Privacy: Emerging Research Priority.... Paradigm of Cybersecurity Research

- **Prof. Virendra Sule** – Professor Electrical Department IIT Bombay, Mumbai
- **Prof. Veni Madhavan** – Professor, IISc Bangalore
- **Mr. Mika Susi** – Executive Director at Finnish Information Security Cluster (FISC), Finland

Moderator: Prof. Jaideep Srivastava– Professor, Data Science, Director of Undergraduate Studies, Department of CSE, University of Minnesota

IITB, Mumbai

IISc Bangalore



Finnish Information Security Cluster, Finland

University of Minnesota

Moderator

In this session, the panelists discussed how we require extensive research to evolve cybersecurity solutions that cater to various organizations' emerging use cases. This need has been amplified by rapid digitization and adoption of technologies such as IoT, ML, AI, etc.

Cybersecurity should be viewed as an enabler for doing things better and not just for protection. The changing societal behaviour towards digital is leading to enormous personal data being collected for personalization and convenience. This leads to apprehensions around privacy with threats fuelled by bad actors, private corporations, government, and even deploy technologies like

ML in chatbots. In this age of corporate espionage, IPR protection becomes a priority. Collaboration between government cyber commands and intelligence sharing between CERT teams or similar agencies is required to avoid a digital meltdown. The panel members deliberated extensively on quantum computing's emergence and significance and how quantum computing can be divided into quantum race and supremacy, quantum readiness, preparedness, and correctness. The looming threat to cybersecurity is that quantum computing would solve all semi-hard (not np-hard) problems on which public-key cryptography is based. Even in the symmetric key area, it may not efficiently solve all problems, but the risks are far too significant. This gives rise to quantum cryptography, a new playground for entrepreneurial and academic talent. Developments in this space would require interfacing with existing systems, PKIs (Public Key Infrastructure), IPsec protocols, and networks. Cryptanalysis, which was used to estimate the security of primitives like symmetric and public-key encryption, became saturated after standardization of the algorithms like AES and key size (256 bits). The rise of quantum compilation means using factorization, brute force, and linear algebra techniques are making encryption standards less prominent and irrelevant. Standardization of post-quantum cryptography is an emerging field in cryptanalysis. Creating and establishing trust, collaboration at a national and international level, a flourishing industry, strong national competencies, and skills form the base ground for digital systems and are likely to require extensive research in the future.

National Strategies for Cyber Education & Skills Building.... Need of Concerted National Action

- **Prof. Rajendra Raj** – Department of Computer Science, Golisano College of Computing and Information Sciences, Rochester Institute of Technology
- **Ms. Danielle Santos** – Manager of Communications and Operations, National Initiative for Cybersecurity Education (NICE)
- **Maj. Gen. Manjeet Singh** – Joint Secretary, Office of National Cyber Security Coordinator New Delhi

Moderator: Mr. Vijay Thadani MD and co-founder NIIT

The distinguished panel elaborated on learnings from global initiatives as well as lessons obtained while implementing such initiatives. They also recommended putting forward ideas, proposals, and frameworks that find a place in the nation's strategy.

The National Initiative for Cybersecurity Education (NICE) program in the USA has gained recognition worldwide. The NICE framework uses an approach consisting of building blocks to define cybersecurity education. This approach focuses on the creation of tasks needed to perform various cybersecurity functions. The program also maintains a repository to list people who are undertaking cybersecurity education and map them with the industry's needs. Thus, it helps employers find employees who have skills in cybersecurity. India is fast emerging as a cybersecurity hub and has the largest talent pool in the world and extremely vibrant economic activity and can undoubtedly leverage learning from a global program such as NICE. From a National cybersecurity perspective, it is extremely important to secure the digital economy, and hence cybersecurity has been a key imperative for the country. At the same time, there has been a surge in cybercrime in the country, and there is an urgent need to ensure necessary cybersecurity know-how and awareness is spread at a mass level. India's National cybersecurity strategy 2020 is currently under development. One of the vision statements is to ensure a safe and secure environment for the nation so that every citizen feels secure from damage due to cyber-attacks and the precautions needed to prevent being victims of cyber fraud. Cyber education and skill development are the fundamental pillars in shaping the cybersecurity education of any country. India is a powerhouse in terms of the number of IT professionals; however, we need more cybersecurity professionals. We may need to re-skills and reorient the available pool of IT professionals. Education and awareness are key for personal safety, and this needs to be understood by the workforce, academia, and the government. If we talk of institutional level, we need to produce a sufficient skilled workforce for the country and map likely avenues of cyber skills in each sector. We need to build globally recognized certification programs.

Further, cybersecurity and cyber education must start at the primary school level. Cybersecurity wellness counseling should be started at the school level to guide students about career options in cybersecurity. We need to have cyber law and cybersecurity education focussed courses at the graduate and postgraduate level. A national cybersecurity skill repository called 'Tech Sagar' developed by DSCI needs to be leveraged and expanded. In India, we are lucky enough to have a national cybersecurity coordination agency and a national cybersecurity skill registry that can be used to create a map of skills and job opportunities in the country. Overall, the revised national cybersecurity strategy looks poised to lead Digital India in a protected and secure manner.

SERI

Security Education, Research, & Innovation Conference

Promoting Cybersecurity Education, Research and Innovation

Get in touch with us

Address : 3rd Floor, NASSCOM Campus, Plot No. 7-10, Sector 126, Noida, UP -201303

Email : ncoe@dsci.in **Contact** : +91 2598 987451