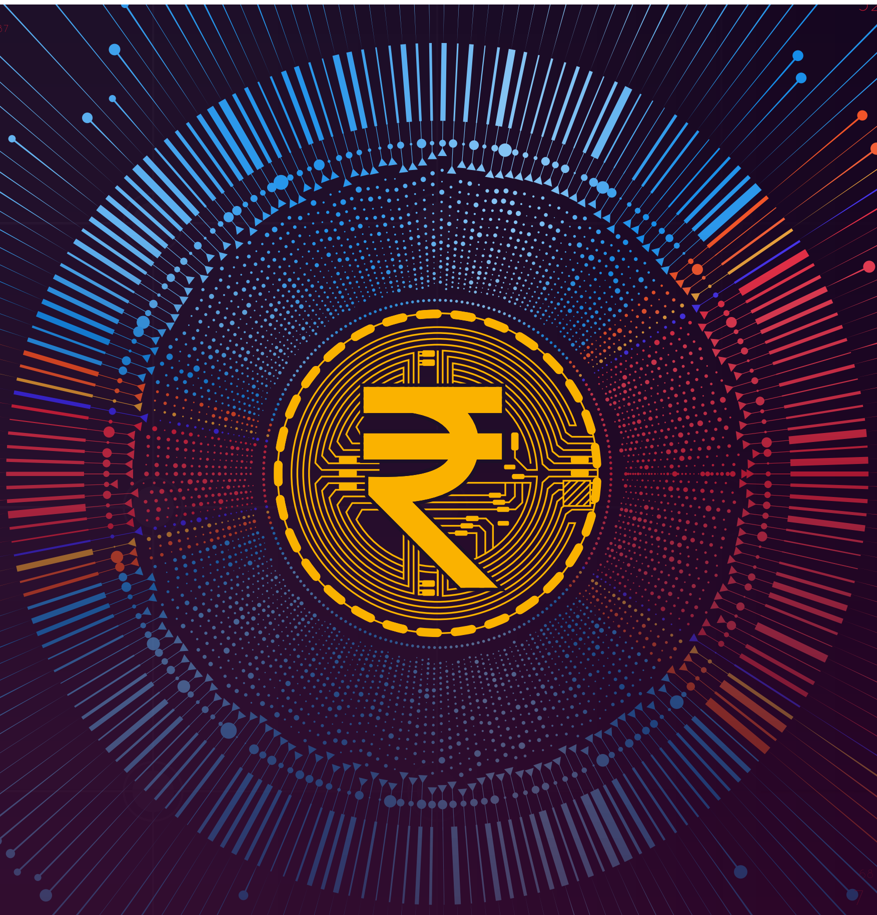
DSCI

PROMOTING DATA PROTECTION

FINSEC CONCLAVE 2023

EVENT REPORT



www.dsci.in/finsec-2023

25-26
MAY 2023

JW Marriott
JUHU, MUMBAI

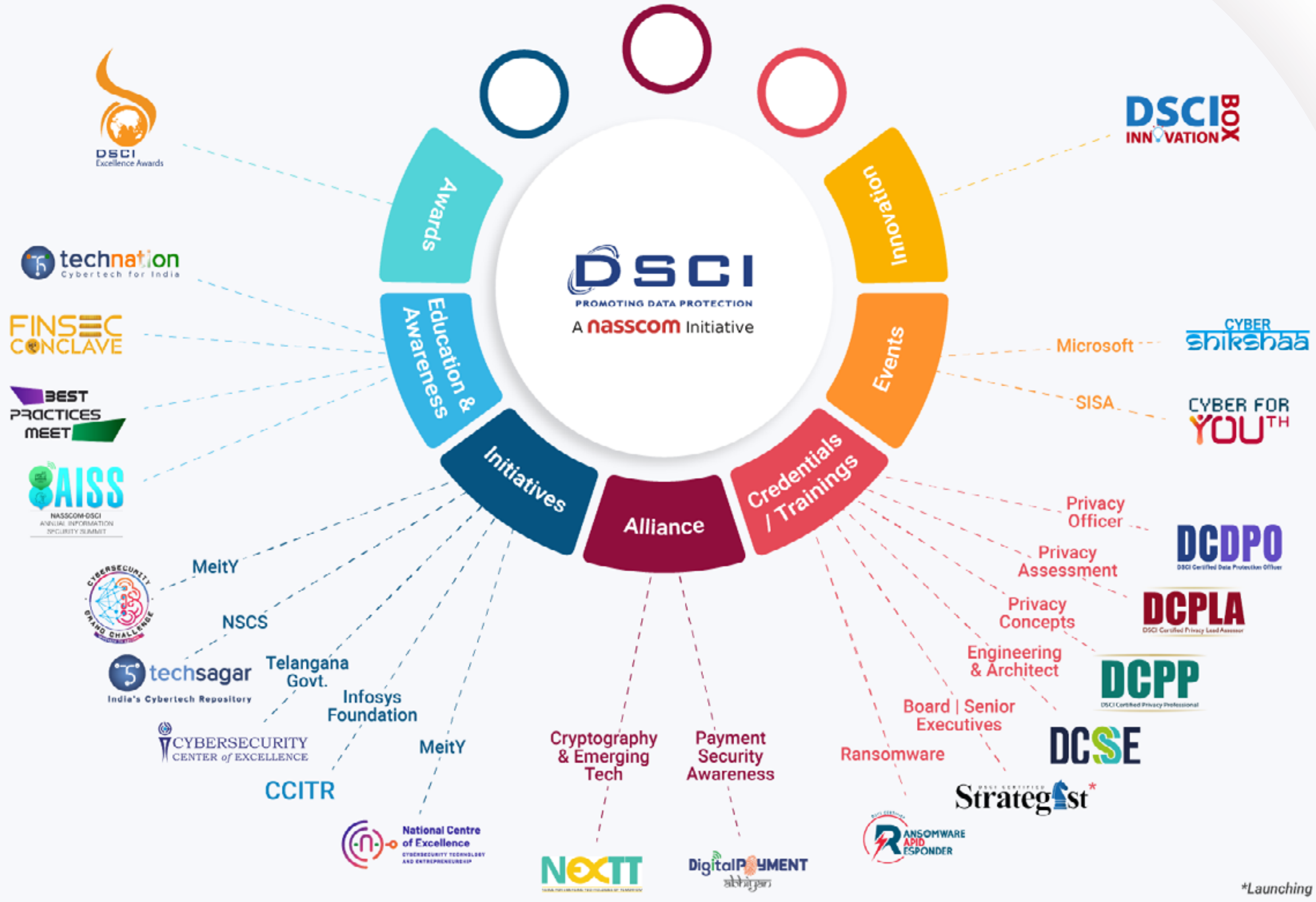
#FINSEC2023
DSCI

Table of Contents

About DSCI

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by Nasscom®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the government and their agencies, Law Enforcement Agencies (LEA), industry sectors including IT-BPM, BFSI, CII, telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

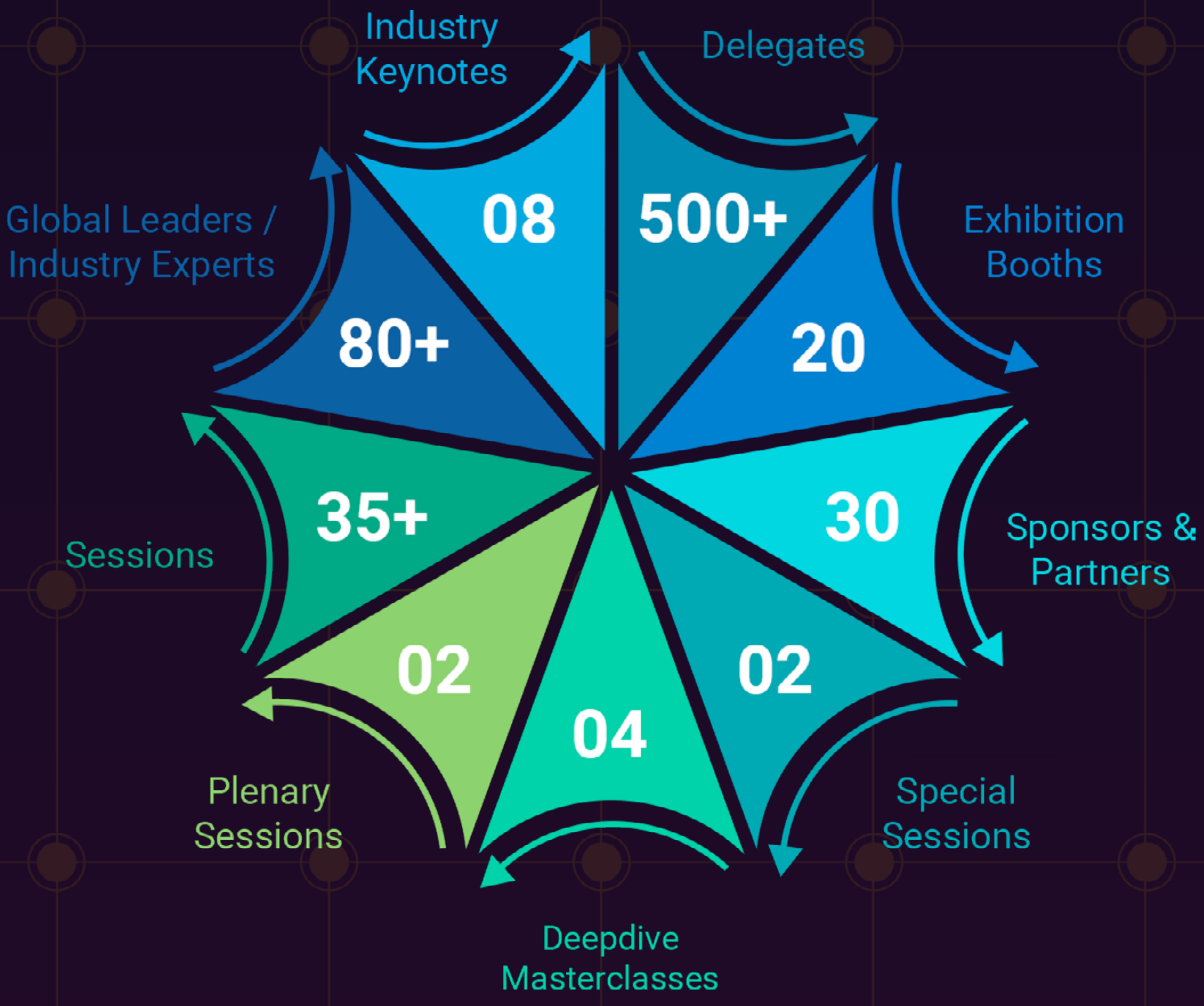
For more information, visit: www.dsci.in



About FINSEC 2023

As the country moves closer to adopting its first comprehensive Data Privacy legislation, financial services organizations are increasingly focusing on preparedness and implementation of Privacy measures. FINSEC 2023 will significantly emphasize Data Privacy and Protection, aiming to highlight best practices that support the Privacy journey within the financial ecosystem. The event will provide an in-depth look at Data Privacy & Data Protection across various sectors, bringing together stakeholders from Banking, Mutual Funds, Securities, Insurance, and Pension to discuss sector-specific preparedness and challenges. Over two days, discussions will cover a wide range of topics including financial frauds, consumer trust, digital resilience, Decentralized Finance, and more, all aimed at addressing the Cyber Security landscape and the technological changes driving digitization and raising Security & Privacy issues within the BFSI sector.

Key Highlights



08 Industry Keynotes

500+ Delegates

20 Exhibition Booths

30 Sponsors & Partners

02 Special Sessions

04 Deepdive Masterclasses

02 Plenary Sessions

35+ Sessions

80+ Global Leaders / Industry Experts

75%
Conference attendees from Top Metros

56%
Delegates from Large-size Companies

44%
Participants from Mid-size & Startups

56%
Professionals from BFSI & Technology Sectors

43%
Experts from IT/ITeS

53%
CISOs, CIOs, CXOs, VPs, AVPs & Directors

FINSEC - DSCI Innovation Box

Start-up Pavilion

Inaugural Session

During the inaugural session delivered by Mr. Vinayak, the spotlight was on quantum computing's transformative potential across industries, underlining its capacity to revolutionize technology-driven sectors. The session extensively discussed the financial sector's evolution, marking significant milestones through the adoption of mobile banking, digital payments, and blockchain, illustrating the sector's dynamic shift towards advanced technological frameworks. A significant emphasis was placed on the necessity of upholding data privacy, securing personal information, and adhering to stringent data protection regulations amidst growing digital data proliferation.

Furthermore, the discussion ventured into the domain of cybersecurity, examining the need for comprehensive security measures to counteract the increasing sophistication of cyber threats. This necessitated a dialogue on international collaboration, exemplified by the Quad Alliance's efforts in steering global technology policies and fostering a unified approach to cybersecurity challenges.

The burgeoning reliance on emerging technologies, notably the Internet of Things (IoT), was highlighted, stressing the imperative for stringent cybersecurity protocols to safeguard interconnected networks and devices. The session wrapped up by deliberating the Data Security Council of India (DSCI)'s pivotal role in the cybersecurity landscape, facing the dual challenge of navigating evolving threats while seizing the opportunities presented by technological advancements. This comprehensive discussion set a forward-looking agenda for DSCI, emphasizing adaptation and strategic capitalization in the face of the cybersecurity sector's dynamic evolution.

> As we navigate India's rapid financial evolution and the shift towards an inclusive & innovation-driven market, financial security has reached a pivotal point, prompting serious discussions on its implications. This conclave is organized to foster meaningful discussions on cybersecurity advancements, aiming to acknowledge and learn from work in various sectors. With the emergence of diverse security disciplines, a collective understanding is crucial. Amidst these innovations, startups are introducing solutions across all critical technologies, positioning the financial sector as a significant market for these security solutions.

Vinayak Godse
CEO, DSCI

Industry Workshops

Workshop by paloalto NETWORKS

Transforming Security Operations with AI

Workshop by Deloitte.

RegTech compliance for Financial Institutions in India...
Managing your regulatory compliance risk

Workshop by CHECK POINT

Securing Supply Chain of Cloud Native Applications

Workshop by SentinelOne

Enter the Incident War Room (at your own risk)

Special Launches & Initiatives

Banking Guide Launch & Workshop

Sectoral Privacy Project
Insurance Sector Workshop

01 Workshop by Palo Alto Networks

Transforming Security Operations with AI

Tarique Ansari
SE, Lead, West Region,
Palo Alto Networks

Ashish Chalke
System Engineer,
Palo Alto Networks

A Security Operations Centre (SOC) serves as the heart of a company's cyber security infrastructure, continuously monitoring, preventing, detecting, investigating, and responding to cyber threats. Automation can enhance SOC effectiveness, but it must be supported by the right investment in technology and a skilled team. The SOC's success relies on the right strategy, commitment, and execution, along with a deep understanding of the organization's culture. SOC teams also play a vital role in vulnerability management, and the adoption of AI and cloud technologies further strengthens SOC capabilities.

Key Takeaways:

1. SOC is tasked with round-the-clock monitoring, prevention, detection, investigation, and response to cyber threats.
2. It safeguards the organization's assets, including intellectual property, personnel data, business systems, and brand integrity.
3. Effectiveness of SOC is significantly boosted by automation, demanding proper technology investment and a knowledgeable team.t
4. A blend of technical expertise and organizational culture understanding is essential due to human limitations in timely threat detection and response.
5. Successful SOC implementation requires more than treating security as a formality; it necessitates a solid strategy, commitment, and proper execution.
6. SOC is responsible for vulnerability management, identifying and remedying vulnerabilities in systems and networks.
7. Integrating AI into SOC operations involves developing appropriate policies, understanding business process integration, and managing AI technologies with a dedicated team.
8. Confidentiality and sensitive information protection are achieved by restricting access to language models like GPT.
9. Cloud technology adoption facilitates advanced SOC capabilities, utilizing tools such as Endpoint Detection & Response (EDR) and Hybrid Detection & Response (HDR).
10. The pivotal role of SOC involves continuous system and asset security, monitoring, and responding to cyber threats.

Good Data Drives Great AI
750 M
new and unique objects analyzed daily
1.5 M
Detect new and unique attacks that weren't there the day before
DSCI
NSEC
CLAVE 2023

02 Workshop by Deloitte

RegTech compliance for Financial Institutions in India... Managing your regulatory compliance risk

Deloitte.

Presented by:
- Munjal Kamdar, Partner, Risk Advisory, Deloitte India
- Praveen Jonnekere, Sales

Anticipated 14% growth for financial institutions in the coming year, with a focus on their economic role and regulatory compliance. Initially concise, data localization regulations introduced on April 6, 2018, have seen clearer understanding over time. Establishing a compliant payment ecosystem with partners is crucial. The discussion acknowledges transaction and payment networks' roles, compliance needs, and adaptation to regulatory changes. Despite recognition, many banks have lagged in data localization compliance. Financial institutions must comply with data localization, privacy, and various regulations, facing challenges in creating compliant ecosystems. Deloitte notes the importance of holistic approaches to compliance, including cloud security and effective data management. Regular system audits by regulators ensure compliance, with Deloitte assisting in data localization compliance through system audit reports. Continuous compliance, secure data handling, and addressing data localization challenges are key, with tokenization playing a role in digital payments. Compliance considerations include outsourcing and vendor relationships, mindful of upcoming regulations like the ADA.

Key Takeaways:

1. Essential compliance involves best practices, reporting, and stakeholder engagement, including business, legal, audit, and IT groups.
2. Continuous compliance requires framework development, assessments, improvement, dashboard/reporting, and architecture reviews.
3. Compliance is necessary for banks, RBI approved entities, and service providers, with regulators demanding detailed information.
4. Compliance steps include inventory classification, remediation, system audits, localization by design, and tokenization for data security.
5. Outsourcing and third-party risk management are key trends, with evolving regulations and the importance of System Audit Reports (SAR).
6. Strategy, security, vigilance, and resilience are foundational pillars for regulatory compliance, focusing on fintech and supervisory enforcement.
7. Challenges in fintech compliance are addressed through regulatory frameworks, emphasizing objectives, activities, and outcomes.
8. Key areas include exemptions, tokenization, data management, compliance in cloud services, and adherence to RBI guidelines for outsourcing.
9. Deloitte's framework and RBI's guidelines stress robust risk management, monitoring outsourcing, and strategic compliance efforts.

03

Workshop by CheckPoint

Securing Supply Chain of Cloud Native Applications

Presented by:

- Vikas Rajpal, Head of Cloud & Harmony Business, India & SAARC, Checkpoint
- Govil Rajpal, Team Lead Security Engineering, Checkpoint

In their comprehensive analysis, the speakers delved into the realm of cybersecurity, exploring the mechanisms through which it can be effectively implemented. They highlighted the inherent vulnerabilities in software systems that render them insecure, posing significant challenges for application developers. They emphasized the need for a zero-trust DevOps supply chain, highlighting the importance of security keeping up with the rapid pace of development. They identified challenges arising from faster development cycles, where security checks and visibility often take a backseat. In the quest to meet deadlines, developers may inadvertently push out vulnerable code, further exacerbating the risk of cyber-attacks. To address this, they stressed the significance of security teams assisting developers efficiently. Collaboration between security and development teams becomes crucial to ensure that security measures are integrated seamlessly into the development process without hindering productivity. By working together, security professionals can provide the necessary guidance, tools, and resources to help developers prioritize security and mitigate risks effectively, emphasizing the need for bridging the gap and fostering collaboration. Additionally, they shed light on the concept of a breach, where unauthorized access compromises the integrity of sensitive information, citing instances such as exposed API keys, misconfigurations, supply chain attacks and exposed passwords as common culprits.

In a significant shift, the speakers noted that cloud security breaches have now surpassed on-premises breaches. This highlights the reality that data is truly ubiquitous, residing in various cloud environments. They emphasized the emergence of a hyper-distributed workspace, where employees can access and collaborate on data from anywhere. With digital transportation becoming faster than ever, the attack surface has expanded exponentially. Organizations now face the challenge of securing a vast and diverse range of endpoints, networks, and cloud services. This widening attack surface necessitates a comprehensive and proactive approach to cybersecurity, encompassing robust cloud security measures, network security, endpoint protection, and data encryption, among other strategies. It is crucial for organizations to continuously adapt their security practices to effectively address this evolving threat landscape.

The speakers emphasized a crucial principle: the more users a system has, the greater the potential for attacks. To address this challenge, they proposed a comprehensive approach: code, build, test, release, deploy, and operate for security protections. They highlighted the significance of incorporating security checks at every stage of the pipeline, using platforms like GitHub to enforce these measures by communicating, planning, and monitoring. By implementing a code quality gate and securing the pipeline, organizations can establish a robust framework that ensures trust and minimizes vulnerabilities. Furthermore, the speakers emphasized the importance of workload protection, safeguarding critical assets from potential threats throughout the system's operation.

04

Workshop by SentinelOne

Enter the Incident War Room (at your own risk)

Presented by:

- Gaurav Singh, Systems Engineer-West, SentinelOne
- Shanker Sareen, Head of Marketing, SentinelOne
- Srikanta Prasad, Senior Director, Arete
- Bhishma Maheshwari, Senior Vice President, Marsh
- Yashaswi Mudumbai, Senior Director, Solution Engineering, SentinelOne
- Prateek Bhajanka, APJ Field CISO, SentinelOne

Cyber Truths: Debunking Cybersecurity Myths (30 mins)

Incident Theatre- Table Top Exercise (30 mins)

Live Demo: Re-invent your SOC with XDR in Action (20 mins)

05

Banking Guide Launch & Workshop

Presented by:
- Varun Sen Bahl, Manager Policy, NASSCOM

Banking Guide Launch at FINSEC 2023: Varun Sen Bahl, Manager of Policy at NASSCOM, unveils an indispensable resource for navigating the evolving landscape of financial security. This session showcases the latest insights and strategies essential for the future of banking.

POLICYHOLDERS' JOURNEY

From the point of searching for an insurance service to the time of exit, the customer's journey includes a number of steps that lead to the generation of data.

01 Search and Selection

The policyholder searches for insurance options, compares em, and selects the preferred urance plan. A proposal form filled out during this stage.

02 Onboarding

The policyholder gives consent for data processing and provides personal information. A KYC form is filled out to verify the details. The ISP independently assesses the risk based on the profile.

03 Purchase and Use

Once the insurance contract is approved, it is sent to the policyholder via email or dispatch. Insurance repositories, acting as intermediaries, maintain records of issued policies. Personal data of policyholders is shared with different repositories during this process. The policyholder starts paying regular premiums. If an insured risk occurs, the policyholder can request for a claim.

04 Exit

The policyholder has the option to not renew the insurance policy.

06

Sectoral Privacy Project... Insurance Sector Workshop

Presented by:
- Srikara Prasad, Research Associate, Dvara Research

Plenary & Special Sessions

Plenary Session

Vision 2025: Digital Payment

... Security and privacy agenda for Contactless, Interoperable, Contextual, Resilient, & Global vision

Plenary Session

Financial Sector and Ransomware

... Blueprint for preparedness and response

Special Session

Decade of Authentication

... Cryptography enabling new digitization possibilities

Special Session

Cyber Maatrika - an initiative to build model specifications

01

Plenary Session

Vision 2025: Digital Payment

... Security and privacy agenda for Contactless, Interoperable, Contextual, Resilient, & Global vision

Key discussion areas:

1. In today's world, the digital economy is a major driver of economic growth and innovation, but it also brings with it new and complex challenges. As more and more of our economic activity becomes digital, it is important for businesses and individuals to be aware of the potential risks and take steps to protect themselves and their assets. Digital risks, on the other hand, refer to the risks and challenges associated with the use of digital technologies in the economy. These risks can take many forms, including cyber-attacks and data breaches, online fraud and scams, and the unauthorized access or use of personal data.
2. Assets were owned then; they are shared now. Competition was owned then; it's unpredictable now. Innovation was methodical then; it's rapid now. App-deployments was timely then; it's instantaneous now. Organizations were built to last then; they are built to change now.
3. Three buckets of adversaries – typical e-crime actors whose motivation is primarily financial gains, state-sponsored actors that have geopolitical reasons and typical hacktivists whose motivation is attention via disruption with no financial gain motives.
4. The average time that an adversary takes all the way from initial axis, persistence, lateral movement and finally data exfiltration is anywhere between 98 to 100 minutes.
5. About 80-90% breaches have threat actors exploiting MFA in external facing applications and user systems, not restricting access privileges, not patching external facing applications due to pathing syndrome or pathing fatigue and not restricting, alternate remote management tools and not having adequate offline backups in common.

Moderator:

- Vinayak Godse, CEO, DSCI

Speakers:

- Nandkumar Saravade, Advisory Board Member, 1Kosmos
- Sreeram Upendran, Vice President Engineering - Asia Pacific Technology, American Express
- Nitendra Rajput, Senior Vice President, AI Garage, Mastercard
- Praveena Rai, Chief Operating Officer, NPCI

02

Plenary Session

Financial Sector and Ransomware

... Blueprint for preparedness and response

Ransomware, exploiting encryption to hijack data, has escalated the financial sector's risk, growing its market from $350 million to an alarming $40 billion. Despite this, the importance of preventative measures like tabletop exercises is often underestimated. Ransomware typically infiltrates through phishing or compromised data, necessitating asset categorization and improved system monitoring for prevention. Surprisingly, 30% of attacks start with unaware lower-level employees. Thus, enhancing email security, ensuring employee training, and mental stability are crucial. Advanced Detection and Response (ADR) systems and robust backup solutions are essential for detecting threats and ensuring recovery, underscoring the need for serious attention to ADR alerts and comprehensive defense strategies.

To further enhance ransomware defense, organizations in the financial sector must also invest in regular security audits and threat intelligence sharing. This proactive approach allows for the identification of new threats and sharing of mitigation strategies among peers, bolstering collective security. Additionally, fostering a culture of cybersecurity awareness throughout the organization can significantly reduce the risk of successful attacks. By integrating these measures with existing strategies, financial institutions can create a more resilient and comprehensive defense against the evolving threat of ransomware.

Key discussion areas:

1. Ransomware's exponential growth to a $40 billion market underscores its significant threat to the financial sector. Tabletop exercises are critical for preparedness and mitigation.
2. Effective defense against ransomware requires more than Indicators of Compromise (IOC); it involves asset classification, segmentation, enhanced monitoring, and software hygiene to prevent vulnerabilities.
3. A significant portion of attacks (30%) originate from less aware lower-level employees, highlighting the need for improved email security, employee training, and mental stability.
4. Utilizing technologies for email attack prevention, taking Advanced Detection and Response (ADR) system alerts seriously, and implementing robust backup systems are essential for resilience against ransomware attacks.

Speakers:

- Darshit Ashara, Head, Security Research, CloudSEK
- Dhananjay Khanna, Sr. Vice President / CISO, SBI Card
- Subba Perepa, MD, JPMC
- Sriram Birudavolu, CEO - Cyber Security, CoE

03

Special Session

Decade of Authentication

... Cryptography enabling new digitization possibilities

The last ten years saw a significant change in the voyage. We examine the significant influence that cryptography has had on how we safeguard our digital identities.

A post-quantum era ready for authentication is one of the topics of consideration. The key to secure connection between cloud and device is disclosed. The talk of data privacy and unique identity security was one of the main highlights.

In addition to discussing the future of cryptography and authentication mechanisms that will open the door to a safer future, panellists offer their thoughts on the regulatory environment, important factors to consider, and implications for secure data protection.

Speakers:

- Ajit Hatti, Founder, PureID
- Manoj M Prabhakaran, Computer Science and Engineering, IITB
- Dr. Ashok Kumar Nanda, Associate Professor, BV Raju Institute of Technology
- Alan Goh, Sales Engineering, DigiCert

04

Special Session

Cyber Maatrika - an initiative to build model specifications

The speakers highlighted various types of technology that play a crucial role in cybersecurity. Additionally, they noted that 31 companies achieved unicorn status in the cybersecurity industry this year, underscoring its rapid growth and importance. However, they identified procurement as a significant challenge, primarily due to unclear license conditions. Establishing clear security targets and defining the skills and roles of Chief Information Security Officers (CISOs) emerged as crucial areas requiring attention. The authors emphasized the need for certifications specific to the CISO role to ensure expertise and competency. They also mentioned the importance of the cyber market's ability to facilitate communication and collaboration among different entities, emphasizing its positive impact. Furthermore, the speakers touched upon the topic of telecom security assurance, where they emphasized the significance of Subscriber Identity Modules (SIM) as the organization's "eyes" and discussed challenges related to defining security requirements in this context. Technological aspects and procurement decisions were also mentioned as important considerations in this regard.

Speakers:

- Narendra Nath Gangavarapu , Director, National Internet Exchange of India
- Manish Nagle, CISO, Equifax
- Vinayak Godse, CEO, DSCI

Industry Keynotes

Supply Chain Attacks in Depth

Speaker: Rahul Sasi, Founder & CEO, CloudSEK

A Collaborative Defense Approach

Speaker: Kaustubh Deshmukh, Director Sales (India Region), Fortinet

Simplifying Security through Consolidation

Speaker: Sandeep Variyam, Cybersecurity Advisor, Palo Alto Networks

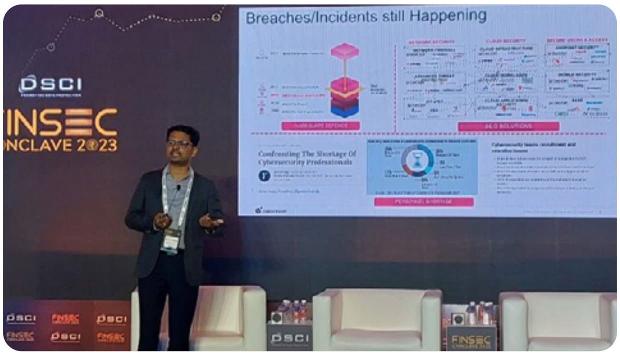
Customer Voice: The Journey to Passwordless

Speakers:

Nandkumar Saravade, Advisory Board Member, 1Kosmos

Mathan Babu Kasilingam, CISO, Ex- CISO NPCI, Vodafone Idea Limited

CHECK POINT™


DSCI
FINSEC
CONCLAVE 2023
Breaches/Incidents still Happening
Confronting The Shortage Of Cybersecurity Professionals

Artificial Intelligence and the Evolving Threat Landscape - Preparing for What's Next

Speaker: Hitesh Pathak, Lead Security Engineering Commercial & Channels segment (India & SAARC) & Office of the CTO, CheckPoint

SentinelOne®

Predict and Protect with Confidence

Speaker: Yashaswi Mudumbai, Senior Director, Solution Engineering, SentinelOne

Prophaze
The New Phase of Security

Application Security Posture Management for Fintech

Speaker: Lakshmi Das, Co-founder and Product Evangelist, Prophaze

OneSpan
The Digital Agreements Security Company

Mobile Banking Fraud Mitigation

Speaker: Pinakin Dave, Country Manager - South Asia, OneSpan Inc

Special Keynotes/Sessions

Special Keynote

Speaker: Sameer Ratolikar, Senior Executive Vice President, HDFC Bank

Special Session

AWS Table-Top Conference

India Cyber Security Trade Mission
New Delhi, Mumbai, Hyderabad, and Bengaluru
May 22-26, 2023

Special Session

Indo-US Cybersecurity Conference

Breakfast Session - Day 1

Ensuring quantum resilience for critical systems

... deliberating the imperatives for post-quantum security

Speaker: Vinayak Godse, CEO, DSCI

Breakfast Session - Day 2

Examining the Generative AI phenomenon from Security standpoint

... gauging the organizational response

Speaker: Aditya Bhatia, Senior Consultant, DSCI

Track Sessions - Day 1

Track Session 1

Digital Identity: Transaction Security & Fraud Management

... Future of Digital Identities

Track Session 2

API Banking and Finance

... How to alleviate security threats and privacy concerns

Track Session 3

Cloud and Compliance

... Devising strategies by comprehending complexities & nuances

Track Session 4

CISO as Digital Business Enabler

... CISO enabling new possibilities for transaction possibilities

Track Session 5

Zero-Trust: Where are you in the Journey?

... What is on the road of journey to the zero-trust?

Track Session 6

Resiliency for Digital Enterprise

... Need to revitalize the resiliency for the digital realities

Track Sessions - Day 2

Track Session 7

Embedded Finance: Next Paradigm

... Strategies for Security and Privacy

Track Session 8

Securing Super App: Aggregating Services and Data

... Identities, Interfaces, APIs, and Data Intermediation

Track Session 9

Taking a sectoral approach to Cyber Security skills

... Addressing the gap in the financial services sector

Track Session 10

Data strategy for financial sector

... Public policies and data governance

Track Session 11

Rising Scale and Potency of Digital Crimes

... Finding matching and effective solutions

Track Session 12

Security Operations and Governance

... Threat Modelling, Trust, and Privacy Trade-offs

FINSEC – DSCI Innovation Box 2023

The DSCI Innovation Box served as a focal point within the esteemed DSCI Excellence Awards 2023, dedicated to celebrating startup excellence and innovation, boasting a rich legacy spanning 13 years. Specifically tailored for FINSEC 2023, this marked the 14th edition of the Innovation Box, spotlighting innovative cybersecurity product companies in the Financial Sector Security realm. This edition was crafted to honour and reward individuals who demonstrated strategic, proactive, and innovative FinTech security solutions, making significant contributions to address real risks, building resilience, and enhancing trustworthiness in the BFSI & FinTech sectors.

The DSCI Innovation box happened during the two-day DSCI Financial Security Conclave 2023 took place in-person at the JW Marriott, Juhu, Mumbai from May 25-26, 2023. The event delved into the security and privacy concerns associated with the digitization of the financial sector, bringing together experts, policymakers, developers, and innovators to share insights as well as best practices. It provided a comprehensive overview of the then-current cybersecurity landscape in the BFSI sector, highlighting opportunities for growth and improvement.

The applicants underwent a meticulous selection process based on eligibility criteria and further evaluation. Shortlisted startups had the unique opportunity to pitch their products on May 26, 2023, in front of Jury and Audience. The judging process involved a combination of jury scores (70%) and audience poll (30%), with winners and runners-up receiving due recognition.

Position	Team Name
Winner	SecOps Solution Protectt.ai Labs Pvt Ltd
1st Runner-up	FourCore
2nd Runner-up	Secure Blink Tech Pvt Ltd

Key Event Speakers

DR. BHARAT SARAF
Director - Head, Privacy,
PhonePe Pvt Ltd

HARSHAD MENGLE
CISO,
Aditya Birla Group

HILAL AHMAD LONE
CISO,
Razorpay

NARENDRA NATH GANGAVARAPU
Director, National Internet
Exchange of India

KALPESH DOSHI
Group CISO,
HDFC Life

LAKSHMI H SHASTRY
Principal Architect,
Brillio

PAVITHRA SHWETHA
Vice President,
Wells Fargo Technology

MANOJ M PRABHAKARAN
Computer Science and
Engineering, IITB

PRASANNA LOHAR
CEO,
Block Stack

PRAVEENA RAI
Chief Operating Officer,
NPCI

RAMESH GURRAM
CISO,
Multi Commodity Exchange
of India Limited

COL SANDEEP KHANNA
Director (Information
Security) & CISO,
UIDAI

DR. SANJAY BAHL
Director General,
CERT-In

SHANKER RAMRAKHIANI
CISO,
IIFL Group

SNEHAL KANEKAR
General Manager- Digital
Finance Business,
Mahindra Finance

SRIHARI KOTNI
VP, CISO,
Pine Labs

VIPIN SURELIA
Chief Risk Officer,
VISA

YUKTI SHARMA
Associate Vice President,
Piramal Capital & Housing
Finance Limited

Event Speakers

AJIT HATTI
Founder,
PureID

ALAN GOH
Sales Engineering,
DigiCert

ANINDYA MUKHERJEE
Senior Sales Engineer,
Rubrik

ANUPRITA DAGA
President, CISO,
YES Bank

ARINDAM ROY
Country Director - India and
South Asia,
SANS Institute, APAC

ASHISH CHALKE
System Engineer,
Palo Alto Networks

DR. ASHOK KUMAR NANDA
Associate Professor,
BV Raju Institute of
Technology

ATUL KUMAR
Lead - Government Initiatives,
DSCI

BHISHMA MAHESHWARI
Senior Vice President,
Marsh

BIKASH BARAI
Co-founder,
Firecompass

DARSHAN CHAVAN
CISO,
Canara Robeco

DARSHIT ASHARA
Head, Security Research,
CloudSEK

DHANANJAY KHANNA
Sr. Vice President / CISO,
SBI Card

DHRUVA GOYAL
Founder & CEO,
BugBase

GANESH AR
CISO,
ICICI Bank

GAURAV SINGH
Systems Engineer-West,
SentinelOne

GOVIL RAJPAL
Team Lead Security
Engineering,
Checkpoint

HITESH PATHAK
Lead Security Engineering
Commercial & Channels
segment (India & SAARC) &
Office of the CTO, CheckPoint

KARTHIK RAO BAPPANAD
Head CySecK,
Government of Karnataka

KARTIK SHINDE
Partner | Africa, India
& Middle East (AIM) |
Consulting, EY

KAUSTUBH DESHMUKH
Director Sales (India Region),
Fortinet

KUSH WADHWA
Senior Director,
Alvarez & Marsal

LAKSHMI DAS
Co-founder and
Product Evangelist,
Prophaze

MAHESH AATHAWALE
Partner,
SK Vestigium LLP

MAKESH CHANDRAMOHAN
CISO,
Aditya Birla Capital Ltd

MANIKANT R SINGH
CISO,
DMI Finance

MANISH MIMANI
Founder & CEO,
Protectt.ai

MANISH NAGLE
CISO

MANOJ KUMAR SHRIVASTAVA
CISO, Future Generali India
Insurance Company Limited

MATHAN BABU KASILINGAM
CIS0, Ex- CISO NPCI,
Vodafone Idea Limited

MITHILESH SINGH
Global head - Technology
Audit, Cyber & Analytics,
S&P Global

MUNJAL KAMDAR
Partner, Risk Advisory,
Deloitte India

NANDKUMAR SARAVADE
Advisory Board Member,
1Kosmos

NILESH SANGOI
CIO,
Fincare Bank

NINAD VARADKAR
CISO,
Edelweiss Financial Services
Limited

NIRANJANKUMAR UPADHYE
SVP - Fraud Risk
Management, Hitachi
Payment Services Pvt Ltd

NITENDRA RAJPUT
Senior Vice President,
AI Garage,
Mastercard

PAWAN CHAWLA
SVP and CISO,
Tata AIA

PINAKIN DAVE
Country Manager -
South Asia,
OneSpan Inc

PRASHANT CHOUDHARY
Partner Technology
Consulting, EY

PRATEEK BHAJANKA
APJ Field CISO,
SentinelOne

PRIYA MADHAVAN
Consultant SSC,
NASSCOM

R VIJAY
CISO,
Indian Bank

RADHESH WALWADKAR
Manager - System
Engineering Advance
Technologies for India &
SAARC, Fortinet

RAHUL RAJENDRA PRASAD
Data Privacy Officer,
HDFC Bank

RAHUL SASI
Founder & CEO,
CloudSEK

GOUDA RAJU
Delivery Head IT and
Information security,
Allianz Technology

RAKESH KUMAR KUNWAR
National Sales Manager
- Identity and Access
Management, OpenText
Cybersecurity

S. S. SARMA
Director,
CERT-In

SAMEER RATOLIKAR
Senior Executive Vice
President,
HDFC Bank

SANDEEP KAMBLE
Founder and CTO,
SecureLayer7

SANDEEP VARIYAM
Cybersecurity Advisor,
Palo Alto Networks

SHANKER SAREEN
Head of Marketing,
SentinelOne

A SHIJU RAWTHER
Head - Information
Technology,
SBI Mutual Fund

SIDDHARTH GANDHI
COO-APAC,
1Kosmos

SIDDHARTH VISHWANATH
Risk Consulting Partner,
PWC

SREERAM UPENDRAN
Vice President Engineering - Asia Pacific Technology, American Express

SRIKANTA PRASAD
Senior Director, Arete

SRIKARA PRASAD
Research Associate, Dvara Reseacrh

DR. SRIRAM BIRUDAVOLU
CEO - Cyber Security, CoE

STEVE DSOUZA
Vice President & CISO, ICICI Lombard General Insurance Company Ltd

SUBBA PEREPA
MD, JPMC

SYED SHAHRUKH AHMED
Co-Founder & CTO, CloudSEK SVigi

TARIQUE ANSARI
SE Lead,West region, Palo Alto Networks

VARUN SEN BAHL
Manager Policy, NASSCOM

VIKAS RAJPAL
Head of Cloud & Harmony business, India & SAARC, Checkpoint

VINAYA SATHYANARAYANA
Senior Director - Product Management (Zero Trust and Data Privacy CoE), Quick Heal

VINAYAK GODSE
CEO, DSCI

CDR VINAYAK SRIMAL (RETD.)
Senior Vice President, Kotak Mahindra

VISHAL PRANJALE
Vice President, Cyber Security, Cloud4C Service

VISHAL SALVI
CISO & Head of Cyber Security, Infosys

YASHASWI MUDUMBAI
Senior Director, Solution Engineering, SentinelOne

Sponsors, Partners & Exhibitors

EXCLUSIVE PARTNERS

Supply Chain Intelligence Partner

CloudSEK

Cybersecurity Partner

paloalto NETWORKS

PLATINUM SPONSORS

1KOSMOS

FORTINET

INGRAM MICRO

GOLD SPONSOR

SentinelOne

SILVER SPONSORS

digicert

ADWEBTECH

rubrik

SecureLayer7
Time and Again, Securing you

SEQRITE

PARTNERS

Delegate Kit Partner

3rd Eye Techno Solutions Pvt. Ltd.
A Digital Forensics Company

Special Session Partner

aws

Bug Bounty Partner

BugBase

Workshop Partner

CHECK POINT™

Workshop Partner

Deloitte.

Career Empowerment Partner

(ISC)²®

Secure Messaging and Collaboration Partner

NetSfere
Enabling Communication.

Badge & Lanyard Partner

OneSpan
The Digital Agreements Security Company

Associate Partner

ardent
Data privacy simplified and automated.

Associate Partner

Prophaze
The New Phase of Security

Hybrid Workforce Enablement Partner

PROHANCE

Mobile App Security Partner

Protectt.ai

Cybersecurity Skills Partner

SANS | GIAC CERTIFICATIONS

Engagement Partner

threatcop
Security Starts with People

Global Trade Partner

U.S. COMMERCIAL SERVICE
United States of America Department of Commerce

EXHIBITORS

FireCompass

NETWORK INTELLIGENCE
The Digital Security Company

PROGIST | NR

TALAKUNCHI™
DIGI · INFO · SECURITY

NCOE PAVILION

National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

TO DOWNLOAD SPONSOR COLLATERALS **CLICK HERE**

THANK YOU

DATA SECURITY COUNCIL OF INDIA (DSCI)
NASSCOM CAMPUS, 3rd Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

For any queries contact:
P: 0120-4990262 | E: events@dsci.in | W: www.dsci.in