

Cybersecurity for Rail Systems

Challenges, Strategies and Solutions

July 12, 2018, The Imperial, New Delhi

Cybersecurity for Large Enterprises

New Technologies, New Risks

July 25, 2018, The Grand, New Delhi

Cybersecurity for BFSI

Current Practices, Risks and Future Strategies

August 8, 2018, Grand Hyatt, Mumbai

Organisers:

POWERLINE

Indian
Infrastructure

RenewableWatch

tele.net

Smart Utilities

Co-Sponsor:



Supported by:



CYBERSECURITY SERIES

Mission

- With persistently growing incidents of malware, misinformation and systemic cyberattacks, cybersecurity is no longer just an IT issue for enterprises. With the advent of IoT, wearables and sensor devices, the scope of cybersecurity has increased and so has the complexities related to it. As it turns out, everything that has an IP address today is vulnerable to a hack or cyberattack.
- The situation will become more serious as new and emerging technologies such as cloud, internet of things (IoT), machine to machine (M2M) and artificial intelligence (AI) go mainstream. IoT has started transforming the way enterprises operate, with a promise of more revolutionary changes in future. However, the soaring number of connected devices brings with it potential data security risks. In 2017, there have been several global instances of massive DDoS attacks using hundreds of thousands of compromised IoT devices. Industry now predicts that by 2020, over a quarter of identified attacks on enterprises will involve IoT.
- In this context, India's attempts to transform into a digital economy and its thrust on cashless payments have brought the country's cybersecurity preparedness, or the lack of it, into the limelight. The rate of cybercrime in India increased in 2017, with one case being reported every ten minutes. Moreover, cyberthreats have become more sophisticated, causing significant reputational, financial and competitive damage.
- The complex cyberthreat landscape is pushing enterprises to alter their security practices significantly. They are moving away from a prevention-only approach towards one which is more predictive in nature. Preventive security controls such as firewalls, application security and intrusion prevention systems are now being tweaked to add more intelligence to them. Further, enterprises are increasingly investing in the strengthening of detection and response mechanisms.
- Cloud-based models have emerged as an effective way for organisations to manage cyberthreats. The adoption of such solutions ensures scalability, while controlling costs. Moreover, cloud-based security environment is often managed by a specialist a service provider.
- At the policy and regulatory level, India is taking a fairly progressive view as far as cybersecurity is concerned. The government and associated regulatory bodies such as RBI, SEBI, IRDA have taken steps to improve cyber resilience in the country. However, a lot more needs to be done. There is an urgent need for a well-crafted, national-level cybersecurity framework, with focus on critical infrastructure like energy, defence, telecom and space.
- The mission of this conference is to:
 - ❖ Highlight the trends in the Indian cybersecurity space.
 - ❖ Examine the existing and potential issues and risks for enterprises.
 - ❖ Discuss the policy needs and requirements, and the way forward.
 - ❖ Explore technology advancements

Organisers

The conference is being organised by India Infrastructure Publishing, the leading provider of information on the infrastructure sectors. The company publishes Indian Infrastructure, Power Line, Renewable Watch and tele.net. It also publishes a series of reports on the infrastructure sector including Power, Oil & Gas, Telecom, Aviation, Roads and Bridges, Ports and Shipping, Railways, Water, Finance and Healthcare. We also organise 50 plus events in India and abroad.

CYBERSECURITY FOR RAIL SYSTEMS (July 12, 2018, The Imperial, New Delhi)

Agenda/Structure:

- ❖ Key Trends, Risks and Vulnerabilities
- ❖ Existing Cybersecurity Frameworks and Current Practices
- ❖ Mitigating Risks I: Railway Signalling, Communications and Control
- ❖ Mitigating Risks II: Reservations and Smart Ticketing
- ❖ Mitigating Risks III: Automation and Driverless Operations
- ❖ Big Data and Cybersecurity Challenges
- ❖ Governance, Response and Recovery Strategies
- ❖ Policy and Regulatory Focus
- ❖ Managing the Cyber Skills Gap in Railways/Metro Rail
- ❖ Global Perspective: Key Learnings and Experience

Target Audience:

The conference is targeted at managers/experts in:

Indian Railways, Metro Rail operators, IR-related organisations, Private container rail operators, logistic firms etc.

The conference will also be useful for:

- ❖ Business and IT professionals involved in cybersecurity
- ❖ Consultants advising buyers of IT security products
- ❖ Government, cybersecurity and law enforcement agencies
- ❖ Think tanks
- ❖ Cyber security technology providers
- ❖ Risk managers, auditors, analysts, etc.

**"Early Bird" discount
ends on June 26, 2018**

CYBERSECURITY FOR LARGE ENTERPRISES (July 25, 2018, The Grand, New Delhi)

Agenda/Structure:

- ❖ Enterprise Cybersecurity Defence: Trends and Threats
- ❖ Emerging Legal Framework and Enforcement: Need for Cybersecurity Laws
- ❖ Enterprise Cloud Security
- ❖ IoT and Automation Vulnerabilities
- ❖ Cybersecurity Strategies, Considerations and Risk Management
- ❖ Role of AI and Big Data Analytics
- ❖ Data Protection and GDPR
- ❖ Cybersecurity Norms for Equipment Manufacturers
- ❖ Governance and Compliance: Challenges for CISOs
- ❖ Cost Implications of Implementing Cybersecurity Solutions
- ❖ Need for Cybersecurity Workforce

Target Audience:

The conference is targeted at:

- ❖ Large Enterprises
- ❖ Business and IT professionals involved in cybersecurity
- ❖ Consultants advising buyers of IT security products
- ❖ Government, cybersecurity and law enforcement agencies
- ❖ Think tanks
- ❖ Cybersecurity technology providers
- ❖ Risk managers, auditors, analysts, etc.

**"Early Bird" discount
ends on July 13, 2018**

CYBERSECURITY IN BFSI (August 8, 2018, Grand Hyatt, Mumbai)

Agenda/Structure:

- ❖ Managing Cybersecurity risks and crimes
- ❖ Regulatory Frameworks for Banking and Insurance Sectors
- ❖ Digital Payments: Threats, Vulnerabilities and Counter-measures
- ❖ New Technologies, New Risks: Spotlight on IoT
- ❖ Security Concerns for Cloud Environment
- ❖ Intelligent Systems: Role of AI, Automation and Big Data Analytics
- ❖ Protecting User Data and Identity: Ensuring Data Privacy
- ❖ Strategies and Solutions: Monitoring, Detection and Response
- ❖ Blockchain for Cybersecurity
- ❖ Building a Cyberdefence Program

Target Audience:

The conference is targeted at managers/experts in:

Banks (Public & Private Sector), Insurance, NBFC's, Capital Asset Firms, Payment Banks, Mutual Funds, Stock Broking, Housing Finance Companies, Micro Finance Institutions, Risk Management Companies, etc.

The conference will also be useful for:

- ❖ Business and IT professionals involved in cybersecurity
- ❖ Consultants advising buyers of IT security products
- ❖ Government, cybersecurity and law enforcement agencies
- ❖ Think tanks
- ❖ Cybersecurity technology providers
- ❖ Risk managers, auditors, analysts, etc.

**"Early Bird" discount
ends on July 26, 2018**

REGISTRATION FORM

- I would like to register for the "CYBERSECURITY FOR RAIL SYSTEMS" (July 12, 2018, The Imperial, New Delhi)
- I would like to register for the "CYBERSECURITY FOR LARGE ENTERPRISES" (July 25, 2018, The Grand, New Delhi)
- I would like to register for the "CYBERSECURITY FOR BFSI" (August 8, 2018, Grand Hyatt, Mumbai)
- I would like to register for **two conferences**
- I would like to register for **all the conferences**

I _____ of _____ enclosing Rs _____ vide cheque/demand draft no.: _____ drawn on _____ dated _____ in favour of **India Infrastructure Publishing Pvt. Ltd** payable at New Delhi.

Please send wire transfer payments to:

Beneficiary	India Infrastructure Publishing Private Limited	Bank Account No.	094179587002
Bank Name	The Hongkong and Shanghai Banking Corporation Ltd	Swift Code	HSBCINBB
Bank Address	R-47, Greater Kailash-1, New Delhi-110048, India	IFSC Code	HSBC0110006

Sponsorship opportunities
are available

Name(s)/Designation (IN BLOCK LETTERS)

Company

Mailing Address

Phone

Mobile

Fax

Email

REGISTRATION FEE

ANY OF THE CONFERENCE

Delegates	INR	GST@18%	Total INR	Total USD
One delegate	15,000	2,700	17,700	295
Two delegates	28,000	5,040	33,040	550
Three delegates	41,000	7,380	48,380	806

TWO CONFERENCES

One delegate	27,000	4,860	31,860	531
Two delegates	50,400	9,072	59,472	991
Three delegates	73,800	13,284	87,084	1,451

ALL THREE CONFERENCES

One delegate	36,000	6,480	42,480	708
Two delegates	67,200	12,096	79,296	1,322
Three delegates	98,400	17,712	116,112	1,935

Delegate fee is inclusive of 18 per cent GST.

Payment Policy:

- Cybersecurity for Rail Systems (There is a 20 per cent "Early Bird" discount for those registering before June 26, 2018),
- Cybersecurity for Large Enterprises (There is a 20 per cent "Early Bird" discount for those registering before July 13, 2018)
- Cybersecurity in BFSI (There is a 20 per cent "Early Bird" discount for those registering before July 26, 2018)

Payment Policy:

- Full payment must be received prior to the conference.
- Payments for "early bird" registrations should come in before the last date of discount.
- Conference fees cannot be substituted for any other product or service being extended by India Infrastructure Publishing Pvt. Ltd.
- Conference fee includes lunch, tea/coffee and conference material.

For registration opportunities, please contact: Naorem Yaiphaba | Conference Cell
Email: naorem.yaiphaba@indiainfrastructure.com | Tel: +91-11-41034610 (D), 41034615, 41034600 (B) | Mobile: +91-9971722464

Conference Cell, India Infrastructure Publishing Pvt. Ltd., B-17, Outab Institutional Area, New Delhi 110016.
Fax: +91-11-26531196, 46038149