Readiness For The Cyber and Data Challenge 2021

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

As most of the people are hooked to their Internet-connected devices for far too longer, cybercriminals are seeing more opportunity to push their agenda and garner profit, resulting in a huge number of ransomware attacks, data breaches, and even very sophisticated nation-state sponsored attacks.

Venue: Virtual Event

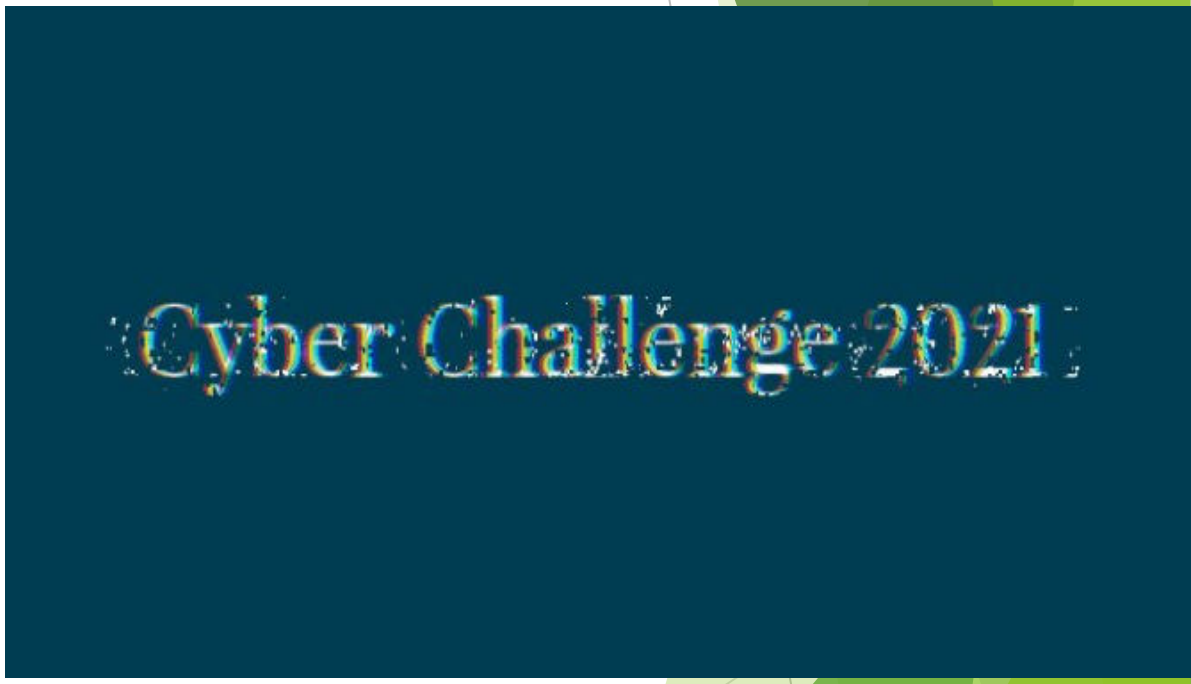
Cyber-crime is a massive business opportunity for the hackers

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

Cyber-crime is a massive business opportunity for the hackers and they put huge effort before launching any cyber-attack.

One of the biggest trends we foresee in the coming year is around building a connected and intelligent world. The emergence of devices that are not only connected but are able to take informed decisions based on data is well underway and this trend will largely be defined by four pillars -

- **Connectivity** - The fourth industrial revolution will be built on 5G, which will be driven by convergence of digital and physical technologies such as digital connectivity, cloud and edge-computing, IoT and smart devices, AI, robotics, blockchain, and AR/VR
- **Sensor** - While more pixels and more cameras will be enhancing the quality of pictures, smart sensors will provide more intelligence and will enable to choose the best shots too. Beyond image sensors, other sensors are also catching up to mimic human capabilities
- **Data** - With big data on rise, storage solutions have evolved from core storage to a hybrid multicloud infrastructure
- **AI** - Artificial intelligence will be critical with movement from Cloud based AI to Edge based AI, to enable real time decision making”



Fifth Generation Technology Standard for Broadband Cellular Networks

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

Rapid technological change has resulted in many aspects of our lives being connected and affected by digital communications. 5G networks are already going up and Reliance Jio has confirmed that they will be rolling out their 5G networks by the end of the next year. The 5G networks will operate on greater bandwidth allowing for download speeds close to 10 gigabits per second.

The enormous speed of data transfer will usher in an era where the network will operate mobile phones, laptops, desktops and gaming consoles and make virtual reality and augmented reality a part of everyday life. But the most important impact of 5G in consonance with the implementation of Internet Protocol version 6 (IPv6) will be allowing complex machine learning applications that depends on real-time access to big data sources conducted through automation in the field to become a reality and kick-starting an Internet of Things revolution.

The implementation of 5G networks will also be the first step towards creating an era of vehicle automation, driverless cars, drone surveillance and advanced robots that will take up more complex functions.

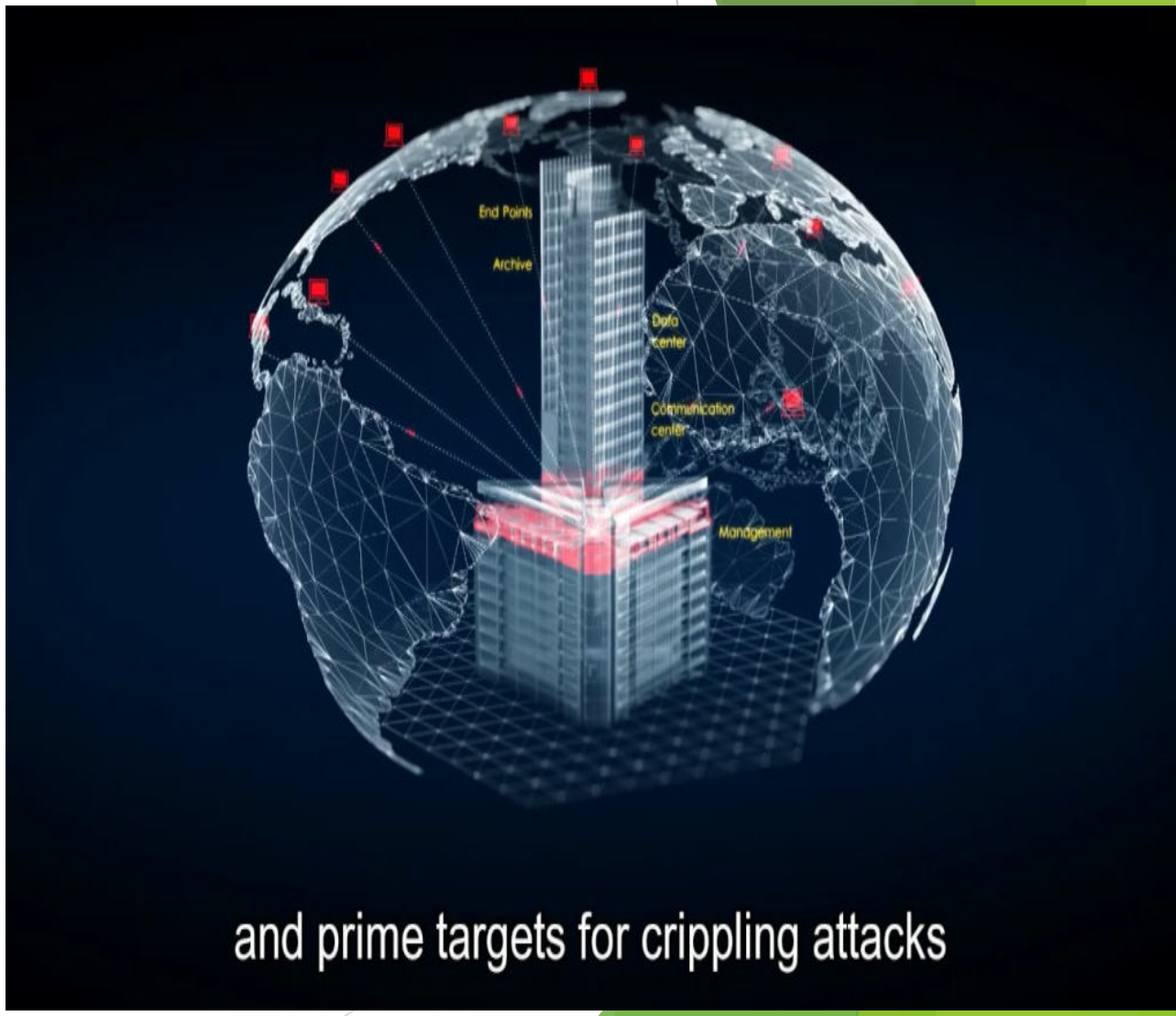
The rise of hyper-automation including (RPA) ,which is the smart packaging of automation tools with embedded cognitive abilities and intelligence. Will it replace several humans in jobs.

Going forward….

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

Cloud technology is here to stay. The Covid lockdown was a demonstration of the power of cloud networks which allowed organisations to shift to alternate work habits without facing major disruptions. The coming year should see cloud providers move towards providing more security and integrations of services to support business units. Cloud servers will also see more applications being run like Machine Learning programs. Cloud computing is in effect, the centralisation of data.

Cyber security is an increasingly important domain today. Countries across the world are concerned about breaches of cyber security which could prejudicially impact their sovereignty and their national security. In this scenario, edge computing is going to bring revolution which allows distributed networks that are closer to the user. In the beginning, edge computing will be used more for running ML programs on aggregated data from a large number of devices but I predict that very soon it will become the next step up the ladder for organisational network architectures.



Cyber security - key challenge for every OEMs

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

There is a global concern on increasing cyber-attacks as more and more organisations moved into a Work From Home (WFH) model and more individuals went on the internet for their social interactions and entertainment. As our personal data including access data for our finances move into cyberspace, the threat of cyber-attacks will only increase.

It is even more worrisome due to the use of non-state actors by rogue nations like Russia, China and North Korea in carrying out concerted acts of cyber terrorism affecting critical infrastructures and financial networks. In the absence of well-defined international treaties that delineate cyber-attacks from an all-out cyberwar, nations will find it difficult to react proportionately.

This year will also see more acts of cybercrimes in the financial space as people will go online for their purchases, thus establishing the cyber trail to be picked up by criminals. As per the recent report, China is targeting all the e-commerce buyers in India.

The aggregation of data due to migration of cloud also creates targets for focussed attacks due to which it is expected that more cloud servers will come under attack. This year should also see a growing number of nation-states come together to counter the menace of cybercriminals.

Right investment into technology will significantly reduce cybersecurity risk

- Employees working from home, office, and other locations (even outdoors) are using company devices and personal devices. Employees are accessing or transferring documents from location to location and device to device, sharing documents with other employees and third parties. Hackers systematically probing networks are seeking to take advantage of new vulnerabilities.
- The hybrid workplace poses enormous cybersecurity challenges for organizations of all sizes. People need to develop new habits and organizations need to implement policies adapted to the hybrid workplace. Human behavior is the foundation of security in all organizations.
- However, organizations also need to consider deploying new technology for the hybrid workplace. As employees move from location to location, they may be using different devices. They are likely using different connections to access your network and data from different locations. Variable access throughout the hybrid workplace creates vulnerabilities and the potential for confusion and chaos.
- Lets understand from the technology leaders how to secure the hybrid workplace in terms of devices, connections, and data.
- **All your basic questions shall get answered in the daylong session**

Tentative agenda(Six tracks of panel discussions)

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

9:00 –10:00-Opening Remarks on *Can India lead in this space ….*
10:00 -10:15 – Welcome address
10:15 -10:30 – Industry address
10:30 -10:45 – Theme address
10:45 -11:00 – Fireside chat

Plenary Session-1(11.00 am to 12.00 Noon)
Panel discussion with the leaders from BFSI

Session-2- (*12:00 Noon to 1:00 pm)*
Panel discussion with the CIO from the IT & ITeS Sector

Session-3 (2.00 PM to 3.30 PM)
Panel discussion with the sSnior Judiciary & Police Officials

Session-4 (*04:00 – 05:00 pm*)
Panel discussion with the Automotive and Hospitality

Session-5 (*06:00 – 07:00 pm*)
Panel discussion on the Readiness of the CISO

Session-6 (*08:00 – 09:00 pm*)
Panel Discussion with the VARs focused into cyber security

Key Take-aways:

1. Unique platform to showcase tech innovation
2. No matter what approach to technology you choose, remember that human behaviour is critical in developing a cyber ready culture at your organization.
3. As ransomware will remain a problem and customers want help to consolidate security tools, corporates and experts are going to explain .
4. 2021 will be a year of consolidation for the cyber security channel, and there will be more merger and acquisition activity, Lets explore more from the experts.
5. In 2021, cyber attackers will increasingly target home routers, insecure IoT devices and VPN systems to infect corporate machines connected to that network, hence this event is going to bridge the gap of demand and supply.
6. Passwords have long been declared defunct. But when it comes to online transactions, they still continue to be heavily relied on in the form of one-time passwords aka OTPs. Hence, consolidation of security tech will be a key opportunity for partners in 2021.
7. Lastly, as businesses undergo digital transformation, whether they migrate to the cloud, leverage next-generation SD-WAN capabilities or see a significant proliferation of IoT devices, there is far more to secure, this brings an opportunity for both vendor and partner eco-system.

Businesses are suffering from cyberattacks

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

The Target Audiences :

. Government Agencies
. Cyber security vendors
. Network solution providers
. Independent software vendors
. Consulting firms
. System integrators
. Value-added resellers
. IT security agencies
. Managed Security Service Providers (MSSPs)

Service :

- Managed services
- Professional services
  - Consulting
  - Training and education
  - Support and maintenance
  - Design and integration
  - Risk and threat assessment

Key Solutions :

. Identity and Access Management (IAM)
. Risk and compliance management
. Encryption
. Data Loss Prevention (DLP)
. Unified Threat Management (UTM)
. Next Generation Firewall
. Antivirus/antimalware
. Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)
. Security and vulnerability management
. Identity and Idea theft managemnet
. Distributed Denial of Service (DDoS) mitigation
. Web filtering
Others .....

Cutting-edge solutions into cyber security

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

Security Type :
Network security
Endpoint security
Application security
Cloud security
Wireless security
Others

Deployment Mode :
Cloud
On-premises

Organization are soft target :
Small and Medium Enterprises (SMEs)
Large enterprises
Government Offices
Courts and shopping complexes

Industry Verticals :
Cyber Defence
Government and PSU
Judiciary & police officials
Banking, Financial Services, and Insurance (BFSI)
IT and ITeS
Hospitality & Retail
Automotive
and Others …

Contact :

Corporate Office -
VAR House
Kalinga Digital Media Pvt. Ltd.
A-84a/3 & 6, Rose Apartments,
Paryavaran Complex, IGNOU Road
New Delhi-110030
Tel. : 011-41656383(10 Lines), 41655458
Fax.:011-46061809
E-mail: publisher@varindia.com
www.varindia.com /www.mybrandbook.co.in

Regional Offices:

Bangalore Mumbai Chennai Kolkata Hyderabad Bhubaneswar