



Proceedings of
**National Conference of
CISOs/CROs and Intermediaries**

September 9, 2021



BUREAU OF POLICE RESEARCH AND DEVELOPMENT
Ministry of Home Affairs, Government of India

Promoting Good Practices & Standards



Proceedings of

National Conference of CISOs/CROs and Intermediaries

September 9, 2021

BUREAU OF POLICE RESEARCH AND DEVELOPMENT
Ministry of Home Affairs, Government of India

Promoting Good Practices & Standards

बालाजी श्रीवास्तव, भा.पु.से.
महानिदेशक

Balaji Srivastava, IPS
Director General

Tel. : 91-11-26781312 (O)
Fax : 91-11-26781315
Email : dg@bprd.nic.in



पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037



Foreword

It is with deep satisfaction that I write this Foreword to the Proceedings of the National Conference of Chief Information Security Officers (CISOs)/Chief Risk Officers (CROs) and Intermediaries organized by the NCR&IC, BPR&D and I4C, MHA jointly on 9th September 2021 at BPR&D Hrqs, New Delhi.

The Police functions in a very dynamic environment wherein the social, religious, political and other factors change rapidly which impact the functioning and efficiency of the police. The easy access to technology, social media, means of communication to the anti-social elements further compound the problem. These new and emerging challenges keep the Police on their toes to deliver new ways and methods for remaining one step ahead of the criminals.

The States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of cybercrimes through their Law Enforcement machinery. However, Cyber Crime Investigation, in a large number of cases, has inter-state and international ramifications and requires an enabling eco-system for successful investigations.

The requirement to keep pace with the rapid modernization of user-friendly technology has been immense to ensure an effective environment for the safety and security of the citizens. The focus now needs to be shifted to innovation, research and capacity building for optimal utilization of human resources.

To meet the challenges of cybercrimes, the Union Home Ministry has rolled out the 'Indian Cyber Crime Coordination Centre (I4C), a scheme to combat Cyber Crime holistically. One of its components, the National Cyber Crime Research & Innovation Centre (NCR&IC) has been assigned to the BPR&D to identify emerging cyber threats and crimes and to proactively find R&D solutions by

"Promoting Good Practices and Standards"



involving various stakeholders, academia/institutions, start-ups and incubation centres.

This Conference is an endeavour to provide a unique platform to the Cyber Security experts and professionals from academia and industries as well as the domain experts in the Government for exploring a robust strategy to tackle the emerging Cyber Security challenges. There were separate sessions on the relevant themes during the Conference, including Critical sector-related Risks and roles and responsibilities of CISO/CRO, Best Practices in Cyber Security, Securing Critical Cyber-Physical Infrastructure and Emerging Trends in Cyber Security.

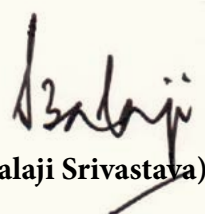
I thank all eminent speakers and participants for their contributions to different Sessions of the Conference.

I record my deep appreciation to Dr Karuna Sagar, IPS, IG/Director, Modernization, Sh. BS Jaiswal, IPS, IG/Director, Training, Dr M M Gosal, Senior Scientific Officer (Traffic & Transport) and Cyber Security Researchers at the NCR&IC, BPR&D, for their outstanding work.

The proceedings of the Conference should be very useful for Law Enforcement Agencies (LEAs) and will go a long way in stimulating new dimensions in Cyber Crime Prevention, Investigation and exploring a robust strategy to tackle the Cyber Security challenges of the new age along with the other stakeholders.

These Proceedings will furnish the States/UTs/CAPFs/CPOs, and other Stakeholders an excellent reference book.

I am also sanguine that this will give an impetus to stimulate further study and research in all these areas.


(Balaji Srivastava)

नीरज सिन्हा, भा.पु.से.
अपर महानिदेशक

Neeraj Sinha, IPS
Additional Director General

Tel.: + 91 11 26781341 • Fax: 91 11 26782201
Email: adg@bprd.nic.in • Website: www.bprd.nic.in



पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037



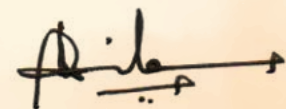
Preface

Developments in the Cyber Space, have had a force multiplier effect on quality of lives of people, across the world. While we count its many blessings, concomitant with it, are deepening concerns of new age Cyber Crime, especially those targeting women and children. Preventing and resolving cyber crimes directed against women and children, remains a singular challenge for Law Enforcement Agencies (LEAs), across the world.

BPR&D, with its motto of 'Promoting Good Standards and Practices', has endeavored to bridge the information gap for the LEAs, with thoughtful seminars and meaningful publications. The National Conference (September 9, 2021) of CISOs/CROs/Intermediaries, coordinated by the Modernization Division, with the help of Professionals of the National Cyber Research & Innovation Centre (NCR&IC), is one of a continuing series of efforts, to reach out to stakeholders spread across.

The Modernization Division Team, led by Dr. Karuna Sagar, IPS, Director, Modernization, Sh. B S Jaiswal, IPS, Director, Training, Dr. M M Gosal, SSO (T&T) and Cyber Security Researchers at the NCR&IC, are deserving of our appreciation for organizing the Conference and publishing the Proceedings.

I trust the Investigating Officers, particularly at the cutting edge, would find the proceedings useful in their professional endeavors, and in helping them combat the demons of new age cyber crime!



(Neeraj Sinha)

"Promoting Good Practices and Standards"

डॉ. करुणा सागर, भा.पु.से.
महानिरीक्षक / निदेशक (आधुनिकीकरण)

Dr. Karuna Sagar, IPS
Inspector General/Director (Modernisation)

Tel. : 91-11-26782023
91-11-26782030 (F)
Email : igmod@bprd.nic.in



पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037



Executive Summary

The National Cyber Crime Research and Innovation Center (NCR&IC), one of the seven verticals of MHA's flagship scheme, Indian Cyber Crime Coordination Center (I4C), is established at the Bureau's Hqrs, New Delhi. NCR&IC is spearheading research and innovation in the areas of cyber crime prevention and cyber security, in collaboration with academia, industry and other stakeholders.

A one-day National Conference of Chief Information Security Officers/Chief Risk Officers/Intermediaries was organised by NCR&IC, BPR&D on 09th Sep 2021. The generous financial support for organising this important conference was provided by I4C, MHA, Government of India.

It is a long standing practice of the Modernisation Division of this Bureau to publish and circulate the proceedings of technical conferences and webinars so that the crucial take-away points of all these sessions reach to a larger audience of States/UTs, CAPF, CPOs and other stakeholders. In this way, the Bureau is continuously involved in circulation of SOPs/Manuals/Proceedings being produced by NCR&IC with regard to emerging cyber security challenges, cyber crime prevention and investigation and capacity building materials for LEAs.

I am immensely happy by offering the Proceedings of National Conference of CISOs/CROs/Intermediaries in your hands. The inaugural session of the conference was graced by Hon'ble MoS (Home), Sh. Ajay Kumar Mishra, Sh. Govind Mohan, IAS, AS (UT), MHA, Sh. Balaji Srivastava, IPS, DG, BPR&D and Sh. Neeraj Sinha, IPS, ADG, BPR&D.

Very distinguished and learned cyber security mentors and experts delved into the range of themes with regard to cyber security.

"Promoting Good Practices and Standards"



National Conference of CISOs/CROs and Intermediaries

There were four technical sessions and a panel discussion encompassing the wide range of topics related to role of CISOs/CROs and Intermediaries in ensuring a safer and secure cyber world.

Technical Session-I was based on the theme “Critical sector related risks and roles and responsibilities of CISO/CRO” and was addressed by Sh. Mohammad Akram Khan, Scientist ‘E’, CERT-In and Sh. Ankit Sarkar, Director, NCIIPC, NTRO.

“Best Practices in Cyber Security” was the theme of Technical Session-II. This session was addressed by Sh. Vikas Tiwari, Head of Solution Architecture – India Central Government, Amazon Internet Services Pvt Ltd, Sh. Vaidyanathan R Iyer, COO, IBM Security Command Asia-Pacific and Sh. Shrikanth Shitole, Vice President & Country Head - India & SAARC, FireEye, Inc.

The third technical session was based on theme “Securing Critical Cyber - Physical Infrastructure” and was addressed by Sh. Rinka Singh, Core Volunteer, iSprit, Bangalore, Sh. Pronab Mohanty, IPS, Deputy DG, UIDAI and Dr. Balsing Rajput, IPS, DCP, Mumbai Police.

Theme of last technical session was “Emerging Trends in Cyber Security” and the various sub-topics under it were addressed by distinguished academics from country’s top research institutes. Dr. Manan Suri, Associate Professor, IIT Delhi, Dr. Arun Balaji Buduru, Assistant Professor and Head - Center of Technology in Policing, IIIT Delhi and Prof Sandeep Shukla, Professor and Head of Computer Science and Engineering Department, IIT Kanpur. The speakers delved at length on Zero Trust Model for Security and Role of Artificial Intelligence in Enterprise Security.

A very enriching panel discussion on a very interesting topic “Industry’s best practices for top cyber threats to an organisation” which was attended by country’s top cyber security mentors. Sh. Brijesh Singh, IPS, ADG (Home Guard), Maharashtra moderated the panel and the panelists included Ms. Rama Vedashree, CEO, Data Security Council of India, Sh. Krishna Sastry, Partner, Ernst & Young, Sh. Vijay Devnath, CISO, CRIS and Dr. Nishakant Ojha, Advisor- Cyber and Aerospace Security.

My colleague, Sh. B.S. Jaiswal, IPS, Director (Training), BPR&D presented a de-briefing talk in which he provided a gist of entire conference and food for thought for all the delegates.

I congratulate the entire team of NCR&IC, colleagues at the Bureau, I4C, the distinguished speakers and the delegates who actively took part in this important conference.

I also extend my sincere thanks to all the government organisations, private firms, academic and research institutes and Law Enforcement Agencies who agreed to nominate their best resources as speakers and panelists in this conference.

(Dr. Karuna Sagar)

INDEX

S. No.	Subject	Page No
1.	Introduction	1
2.	Inaugural Session	2
3.	First Technical Session	4
	Theme: Critical sector related Risks and roles and responsibilities of CISO/CRO	
	Part – I	
	Emerging cyber threats and mitigation measures for CISOs	4
	Part – II	
	Cyber Security in Modern Critical Information Infrastructure	7
4.	Second Technical Session	13
	Theme: Best Practices in Cyber Security	
	Part – I	
	Secure Cloud Services	13
	Part – II	
	Secure Network Infrastructure	23
	Part – III	
	Challenges in Prevention and Mitigation of Cyber Threat	27
5.	Third Technical Session	31
	Theme: Securing Critical Cyber Physical Infrastructure	
	Part – I	
	Secure Online Public/Financial services and Citizens' Data	31
	Part – II	
	Secure online public financial services and citizen data	31
	Part – III	
	New perspective in cyber security for LEAs	34
	Part – IV	
	Cyber physical security and law enforcement agencies	36



6. Fourth Technical Session	38
Theme: Emerging Trends in Cyber Security	
Part – I	
Zero Trust Model of Security	38
Part – II	
AI/ML for Security	41
Part – III	
Artificial Intelligence in Enterprise Security	45
Part – IV	
Artificial intelligence in Enterprise Security	46
7. Panel Discussion	51
8. Debriefing Session	53
9. Glimpses of the Conference	54
10. Contact list of BPR&D officers	72

NATIONAL CONFERENCE OF CISO/CRO & INTERMEDIARIES

9th September, 2021
BPR&D Hqrs, Ministry of Home Affairs, New Delhi

Time	Inaugural Session
0900 – 1000 Hrs	Chief Guest: Sh. Ajay Kumar Mishra, Hon'ble MoS (Home), MHA 0900 - 0905 Hrs: Welcome to Chief Guest & AS (UT), MHA by DG, BPR&D 0905 - 0910 Hrs: Welcome to DG & ADG, BPR&D by IG (Mod), BPR&D 0910 - 0920 Hrs: Welcome Address: Sh. Balaji Srivastava, IPS, DG, BPR&D 0920 - 0930 Hrs: Special Address: Sh. Govind Mohan, IAS, AS (UT), MHA 0930 - 0935 Hrs: Book Release & Prize Distribution to Winners of CTE Contest 0935 - 0950 Hrs: Inaugural Address: Sh. Ajay Kumar Mishra, Hon'ble MoS (Home) 0950 - 0955 Hrs: Memento to Chief Guest by DG, BPR&D 0955 - 1000 Hrs: Vote of Thanks: Sh. Neeraj Sinha, IPS, ADG, BPR&D
1000 – 1030 Hrs	High Tea/Networking
1030 – 1130 Hrs	Technical Session 1 Theme: Critical sector related Risks and roles and responsibilities of CISO/CRO 1030 - 1100 Hrs: Sh. Mohammad Akram Khan, Cert-IN <i>Topic: Emerging cyber threats and mitigation measures for CISOs</i> 1100 - 1130 Hrs: Sh. Ankit Sarkar, NCIIPC <i>Topic: Cyber Security in modern Critical Information Infrastructure</i>
1130 – 1300 Hrs	Technical Session 2 Theme: Best Practices in Cyber Security 1130 Hrs - 1200 Hrs: Sh. Vikas Tiwari, Amazon <i>Topic: Secure Cloud Services</i> 1200 Hrs - 1230 Hrs: Sh. Vaidyanathan R Iyer, IBM <i>Topic: Secure Network Infrastructure</i> 1230 Hrs - 1300 Hrs: Sh. Shrikant Shitole, FireEye <i>Topic: Challenges in Prevention and mitigation of cyber threat</i>
1300 – 1400 Hrs	Lunch Break
1400 – 1500 Hrs	Technical Session 3 Theme: Securing Critical Cyber-Physical Infrastructure 1400 Hrs - 1410 Hrs: Sh. Rinka Singh, iSprit 1410 Hrs - 1430 Hrs: Sh. Pronab Mohanty, IPS, Deputy DG, UIDAI <i>Topic: Secure Online Public/Financial services and Citizens' Data</i> 1430 Hrs - 1500 Hrs: Dr. Balsing Rajput, IPS, DCP, Crime Branch Mumbai <i>Topic: New Perspective in Cyber security for LEAs</i>



1500 – 1600 Hrs	Technical Session 4 Theme: Emerging Trends in Cyber Security 1500 Hrs - 1515 Hrs: Dr. Manan Suri, IIT Delhi <i>Topic: Zero Trust Model for Security</i> 1515 Hrs - 1530 Hrs: Dr. Prathosh A.P, IIT Delhi 1530 Hrs - 1550 Hrs: Dr. Arun Balaji Buduru, IIIT-Delhi 1550 Hrs - 1600 Hrs: Prof. Sandeep Shukla, IIT Kanpur <i>Topic: Artificial Intelligence in Enterprise Security</i>
1600 – 1615 Hrs	Tea Break
1615 - 1715 Hrs	Panel Discussion Topic: Industry best practices for Top threats to an organization - by leading cyber security mentors. Moderator: Sh. Brijesh Singh, IPS, ADG, Maharashtra Panellists: Sh. Krishna Sastry, Partner, EY Ms. Rama Vedashree, CEO, DSCI Sh. Vijay Devnath, CISO, CRIS, Indian Railways Dr. Nishakant Ojha, Advisor, Cyber and Aerospace Security, BECIL
1715 - 1730 Hrs	De-briefing, summing up, Wrap up of the session By Sh. B.S. Jaiswal, IG (Training), BPR&D
1730 - 1745 Hrs	Vote of thanks Dr. Karuna Sagar, IG (Mod), BPR&D



PROCEEDING

NATIONAL CONFERENCE OF CISOs/CROs/INTERMEDIARIES

INTRODUCTION

National Cyber Crime Research & Innovation Center (NCR&IC), BPR&D and I4C, MHA jointly organized the National Conference of CISOs/CROs/Intermediaries on 9th Sep 2021 at BPR&D Hrqs, New Delhi in physical mode.

The CISOs/CROs Conference is an endeavour to provide a unique platform to the cyber security experts and professionals from academia and industries as well as the domain experts in the Government for exploring a robust strategy to tackle the emerging cyber security challenges. There were separate sessions on the following themes during the Conference:

- i. Critical sector related Risks and roles and responsibilities of CISO/CRO
- ii. Best Practices in Cyber Security
- iii. Securing Critical Cyber-Physical Infrastructure
- iv. Emerging Trends in Cyber Security

The event was inaugurated by Sh. Ajay Kumar Mishra, MoS, Home Affairs, Govt of India. Sh. Govind Mohan, AS (UT) also graced the event. Sh. Balaji Srivastava, DG, BPR&D and Sh. Neeraj Sinha, ADG, BPR&D were also present during the inaugural session of the conference.

CISOs/CROs from States/UTs, CPOs and CAPFs and from various ministries like Ministry of Education, Ministry of Railways, Ministry of Defence, Ministry of Power, Ministry of Telecom, MitiY, MSME and many others participated in the conference.



INAUGURAL SESSION

The inaugural session of the conference was held from 9am to 10am.

Dr. Karuna Sagar, Director/IG (Modernisation), BPR&D welcomed all the dignitaries by presenting planters to all.

Sh. Ajay Kumar Mishra, Minister of State, Home Affairs, Govt of India inaugurated the National Conference of CISOs/CROs/Intermediaries at 9am on 9th Sep 2021.

MoS, Sh. Ajay Kumar Mishra Ji in his inaugural address appreciated the active role National Cyber Crime Research and Innovation Center (NCR&IC) and Modernisation Division of BPR&D are playing in the field of capacity building of LEAs to tackle cyber crime and cyber security challenges. He further said that the investigation and prevention of cyber crime is a challenging task. On one hand cyber space has made positive impacts on human lives, it has increased our dependence on cyber technologies and as a result it has also posed security challenges before us. He emphasized on the fact that since cyber space is borderless, we need to make world standards in preparations to fight against cyber crime. Under the guidance of our Hon'ble Prime Minister and Home Minister we are creating a new and robust ecosystem in fighting cyber crimes by even amending the I.T. Act.

Sh. Govind Mohan, AS (UT) while delivering his special address said the internet has led to a great set of inventions and it doesn't have any geographical boundaries. He mentioned that MHA is actively working towards ensuring a safe cyberspace for the country. He said that Indian Cyber Crime Coordination Center, founded in 2018 by MHA, is a special purpose unit to fight cyber crime and cyber security challenges. He further mentioned that Cyber crime reporting portal, launched in 2019, is one of the most significant achievements of I4C. This portal is a citizen centric crime reporting portal. He also mentioned the national helpline 155260 launched by I4C, MHA. This helpline is helping the common citizen in registering financial frauds.

Sh. Balaji Srivastava, DG, BPR&D, delivered welcome address. He mentioned about the activities being undertaken by NCR&IC and Modernisation Division, BPR&D for capacity building of LEAs with regard to cyber crime investigation, digital forensics and cyber crime prevention. He mentioned that Modernisation Division and NCR&IC are spearheading research and development in partnership with leading academic institutions to develop research based tools for LEAs for prevention and investigation of cyber crimes. He apprised the audience about the Capture the Evidence Contest for LEAs organised by NCR&IC. MoS felicitated the top three winners of the contest in the inaugural session.

Sh. Neeraj Sinha, ADG, BPR&D presented a vote of thanks and remarked that data has become a new oil and a robust exercise and preparation is needed to prevent the potential misuse of data.



FIRST TECHNICAL SESSION

»» **Theme: Critical sector related Risks and roles and responsibilities of CISO/CRO**

Part I

»» **1030 - 1100 Hrs: Sh. Mohammad Akram Khan, Cert-IN**

»» **Topic: Emerging cyber threats and mitigation measures for CISOs**

The first technical session was held from 10:30am to 11:30am and was based on the theme “Critical sector related Risks and roles and responsibilities of CISO/CRO”.

Sh. Mohammad Akram Khan, Scientist ‘E’, Additional Director, CERT-In addressed the audience on the topic “Emerging Cyber Threats and Mitigation Measures for CISOs”.

The discussion of Sh. Akram Khan revolved around a brief introduction of CERT-In, cyber threats and threat landscape, real world root causes behind successful cyber attacks, and mitigation measures.

He mentioned that CERT-In was founded in 2004 by Department of IT, and in 2008 it got designated as national nodal agency to perform following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed

While elaborating the three tier activities performed by CERT-In, he further elaborated on following points:

1. Incident Response (Reactive Service)
 - Operating Incident Response Helpdesk on 24X7 basis
 - Evidence collection & incident investigation (specialized cases)
2. Incident Prevention and Security Awareness (Proactive Service)
 - Tracking of Security Threats and Cyber attacks
 - Vulnerability Coordination with vendors and OEMs

- Issuance of Security Alerts and Advisories
- Tailored alerts to CISOs/POCs
- Conducting Security Workshops and Security Awareness Programs

3. Security Quality Management Services

- Promotion of Security Best Practices and Security Standards
- Empanelment of Security Auditors
- Conducting Security Mock Drills
- Implementation of Cyber Crisis Management Plan (CCMP)

Continuing the talk, Sh. Akram enlightened the audience on the three categories of cyber threats viz. National Level Cyber threats, Organisational Level Cyber threats and Individual Level Cyber threats. He explained that as a cyber security specialist moves from individual level to national level cyber threats, the complexity, sophistication and enormity of the attack increases. The national level cyber threats like cyber terrorism, attacks on critical infrastructure and Distributed Denial of Services involve multiple layers of threat response.

Sh. Akram Khan also explained in detail about the threat landscape which may potentially hit the target entities like Manufacturing, Utilities, IT Industry, Finance, Telecom and individuals etc.

While discussing the effect of COVID-19 on cyber security, he went on explaining that Business Continuity Plans (BCP) and incident response plans were inadequate or even non-existent at many places. He also mentioned that pandemic forced everyone to operate in non-standard manner which resulted in increased attack surface. Traditional security measures prior to COVID-19 were not sufficient in the current scenario and it caused delays in cyber-attack detection and response.

Sh. Akram urged the audience to religiously follow the practice of strong to very strong password and staying fully alert from potential phishing and spear phishing attacks. He said that many organizations and entities are still using old operating systems like Windows XP, Windows Vista and Windows-7. Usage of old and outdated operating systems in machines make it highly vulnerable.

He further told the audience that ignoring the security alerts is the most dangerous thing to do. If such alerts are ignored then it may turn a minor incident into a major crisis. He highlighted the bad consequences of incomplete incident response which are responsible for wrong assessment, over reliance on tools, and ignorance of lateral movement of threat actors.

Moving further, Sh. Akram explained about simple mitigation measures. He said that procurement of cyber security technological solutions alone are not sufficient for protecting the organization from potential threats, rather it greatly depends on how well the solution has been implemented into the cyber infrastructure of an entity. He suggested first understanding the use cases of the available technology and customizing it based on the specific requirements. He explained about the swiss cheese model for understanding the accidents and improving safety to enable defense in depth inside the organisation's infrastructure. He urged the CISOs to develop and implement incident

response plans to deal with cyber crises, contingencies, disasters and attacks on IT systems. He listed down five security must-haves for any organization:

1. Inventory
2. Secure Configurations
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Continuous Security Monitoring and Incident Response

Sh. Akram mentioned a paper CERT-In had published under the title Key Roles and Responsibilities of CISOs in Ministries/Departments and Organisations managing ICT operations. He urged the audience to visit the following link to download the paper:

https://www.meity.gov.in/writereaddata/files/CISO_Roles_Responsibilities.pdf

While concluding the talk Sh. Akram mentioned the following areas where CERT-In can help organisations and CISOs in mitigating the risks:

- 24x7 Incident Response Helpdesk
- Alerts and advisories on website and mailing list
- Cyber Threat Intel Exchange Platform
- Cyber Swachhta Kendra (Botnet Cleaning & Malware Analysis Centre)
- Cyber security audits (empanelled auditors)
- Exercises and Drills
- Situational Awareness project

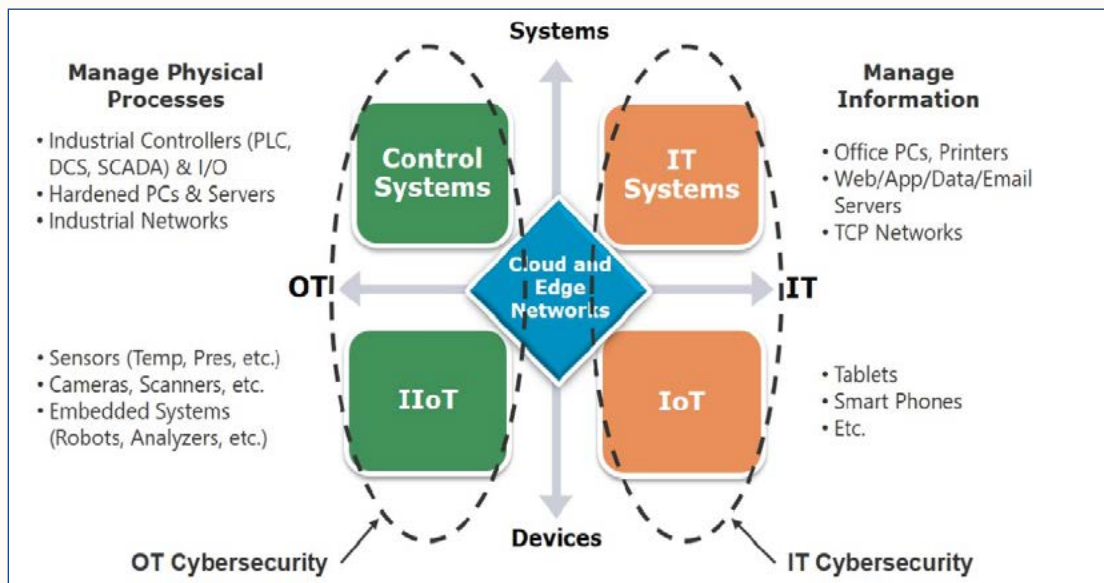


Part - II

» 1100 - 1130 Hrs: Sh. Ankit Sarkar, NCIIPC

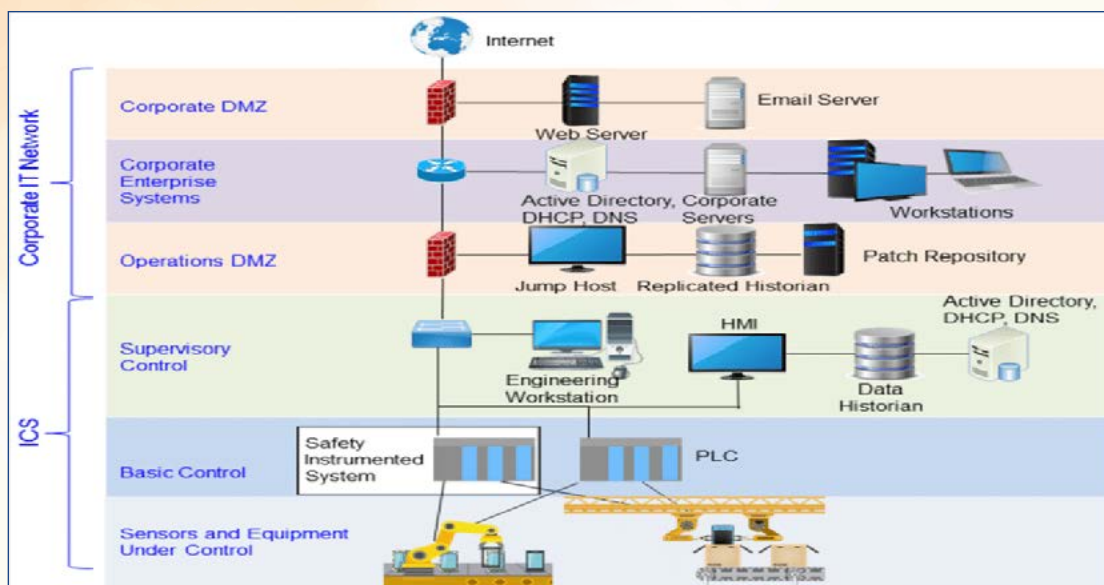
» Topic: Cyber Security in Modern Critical Information Infrastructure

Sh. Ankit Sarkar started his talk by giving an eye bird view understanding of the modern critical information infrastructure. He said that time has come when nobody has to tell us about the importance of cyber security, rather we have already started practicing cyber security. Starting from a home based wi-fi router to a state of art data center, everything falls under the category of information infrastructure. Sh. Sarkar urged on the need of developing an urgent need of realizing the importance of securing our information infrastructure. State of the art data centres to a sewage water treatment facility in a city, everything is running on automation and is critical information infrastructure. To understand the landscape of information infrastructure, following diagram may be helpful:



The image presented above explains how Office PCs to Industrial controllers like SCADA and PLC, Industrial Networks, Embedded Systems used in strategic programs including space missions are connected through cloud and edge networks. Sectors like BFSI, airports and air traffic, water supply systems, road traffic control and monitoring systems, power generation, transmission and distribution systems are all exposed to networks. While explaining about the functioning of NCIIPC Sarkar mentioned that NCIIPC works with various government bodies critical sectors like power, Telecom, rail and air traffic, waterways, telecom and BFSI.

Sh. Ankit Sarkar also explained about the modern critical information infrastructure and how they are functioning at various levels.



Showing the image above Sh. Sarkar described about the critical information infrastructure which is lying inside every organisation. On top of everything there is the Internet under which there is a corporate IT network which is common in all places. Under the corporate IT Network there is a supervisory control layer which essentially is the hardware which communicates with the corporate IT network layer and there is a layer of basic control and sensors and equipment which are the foundation of infrastructure.

Sh. Sarkar also explained about the possible impact of Cyber attack on any critical infrastructure. He mentioned that there can be possibilities like blocked or delayed flow of information, unauthorized changes to instructions, commands, or alarm, inaccurate information to controllers, Malware infection and configuration manipulation. It is the responsibility of CISO and CRO of any organization to properly understand and calculate the vulnerabilities inside the network infrastructure. They are also responsible for estimating the possible damages any cyber attack can cause on the entire system. Modern malware systems are so sophisticated that there is malware always out there for sale for everything and anything. Even a slight delay or blocked flow of information on a critical information infrastructure may lead to huge damage.

The different actors for a cyber attack could be adversarial, accidental, structural and environmental. The adversarial actors may be individual groups Nation states and terrorists. Similarly accidental actors are users and structural actors are IT infrastructure and processes. Lastly the environmental actors can be natural disasters. To prevent Malware entry and its execution there can be several methods which can be adopted by the CISO in an organization who are responsible for securing the critical information infrastructure. The various methods of preventing malware delivery and execution are application whitelisting, patch applications, user application hardening, email and web sandbox, web content filtering, OS exploit mitigation, server application hardening, OS hardening and control removable media.

Application whitelisting helps prevent undesired execution, implementing application whitelisting on important servers such as active directory email servers and other servers handling user authentication can help prevent adversaries from running malware.

Patching of all applications leads to security vulnerabilities in software which enables adversaries to execute malicious code resulting in significant consequences. The level of security risk might also be affected by whether exploit code for security vulnerability is available commercially or publicly for example in an open source tool like the Metasploit Framework or in a cyber crime exploit kit. So as CISO we need to be careful about random application of random patches because not all patches are safe. There should be a comprehensive policy to take timely decisions on whether we can afford the delay of patch application. User application hardening helps in reducing attack surface, it mitigates adversaries using malicious content to evade application whitelisting, avoid exploiting application's legitimate functionality, or exploiting a security vulnerability for which patch is unavailable. We should also think about making our corporate email sandboxing. Email sandboxing is a dynamic analysis technique which uses behaviour based detection capabilities instead of relying on the use of signatures and enables detection of Malware yet to be identified by the cyber security community.

Web content filtering reduces the security risk of Malware being accessed, makes it more difficult for adversaries to communicate with their malware, defining a white list of allowed types of web content assist in removing common Malware delivery techniques.

Operating system exploits should be mitigated. Operating system generic exploit mitigation e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET), Security Enhanced Linux (SELinux) and GRsecurity are examples of exploit mitigation mechanism used for Linux operating systems.

Server application hardening helps the organisation to conduct its business with a reduced security risk of malicious data access, theft, exposure, corruption and loss.

Operating system hardening is a method of facilitating implementing application whitelisting and patching security vulnerabilities. It provides an ability to detect Anomalous software running by monitoring for deviations from the standard baseline. Network administrator knowing what software is running on network devices and what software is permitted to communicate on the network thereby facilitating baselining expected network activity. Ability to quickly restore compromised computers and network devices to a known clean state.

Using removable storage media and connected devices in a controlled and accountable manner reduces the security risk of malware execution and unauthorized data exposure.

We should limit the extent of cyber security incidents by restricting privileges, applying multi factor authentication, performing network segmentation, practicing virtualized sandbox environment and blocking unwanted traffic.

Cyber crime detection incidents and responding mechanisms can be adopted by implementing incident detection and response mechanism, hunting to discover incidents and capturing network traffic. Performing continuous incident detection and response increases the organisation's ability to rapidly detect and respond to cyber security incidents in a timely manner to minimise business impact. A proactive and deliberate activity to discover cyber security incidents by leveraging threat intelligence. Hunting to discover incidents provides an understanding of the adversaries goals, strategy, tactics, technique, procedures and to a lesser extent tools. The focus is not on detecting cyber security incidents based on a list of known malicious domains, IP addresses, file hashes and other indicators of compromise which are similar to reactive signatures. Capturing network traffic can assist the organization to determine the techniques used by adversaries, perform a damage assessment and assist with remediating the compromise.

Data recovery and system availability can be achieved by doing daily backups, maintaining business continuity and disaster recovery plans and regularly updating system recovery capabilities. Proven data restoration processes are vital to mitigate data being encrypted, corrupted or deleted by ransomware or other destructive malware, malicious insiders, accidental mistakes by users, or non-malicious failure of storage hardware due to a change of causes including faulty equipment wear, power outage, fire or flood. Robust business continuity and disaster recovery plans assist with enabling organizations to remain in business and continue providing critical services and products to customers and other stakeholders. System Recovery Capabilities assist mitigating destructive malware, malicious insiders who are motivated to destroy systems, and non-malicious failures of critically important IT equipment.

Personal management assists to avoid employees having malicious intent, developing malicious intent or carrying out their malicious intentions and discovered until after damage has been done.

When an organization decides to move its data on to cloud then it should have following points of cloud framework under consideration:

- Business criticality of data or functionality
- Data backup plan
- Business continuity and disaster recovery plan
- Network connectivity to the cloud
- Vendor's guarantee of availability
- Impact of outages
- SLA inclusion of Scheduled outages

- SLA compensation
- Data integrity, availability and confidentiality
- Data restoration
- Scalability
- Changing vendor
- Handling Cloud Security incident

The Other important points to be taken into consideration under service level agreement are as follows:

- Choice of cloud deployment model
- Sensitivity of data
- Legislative obligations
- Countries with access to data
- Data encryption Technologies
- Media sanitization
- Vendor's remote monitoring and Management
- Data ownership
- Gateway Technologies
- Policies and processes supporting the vendor's IT security postures
- Technologies supporting the vendor's IT security posture
- User authentication
- Vendor's physical security posture

Another method which may be applied by CISO of an organisation is thinking about deploying cyber security deception models. Cyber deception to expose and defeat cyber intruders, APTs and malicious insiders. Active deception proactively applies strategies and actions, malicious actions are anticipated and counter-actions predicted to prevent their successful completion and to misinform them.

Enabling cyber security deception may help the organizations in following ways:

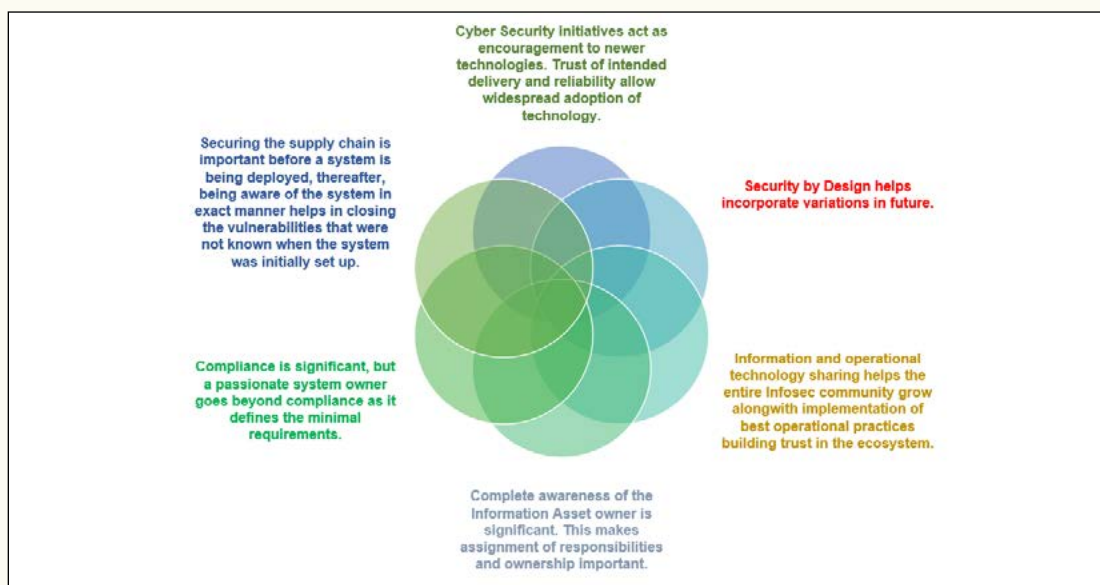
- Increasing entropy of leaked information about kinds of systems targeted
- Gaining information about compromise methodologies
- Enabling Observation, Orientation, Decision and Action (OODA)

Adaptive approach is needed to develop a culture of cyber resilience into an organization.

- Resilience: The ability of an organization to not only prepare for and detect security threats, but to respond effectively in a timely manner, minimize damage, withstand disruptions and to learn and adapt.

- **Detection:** Comprises the learning capabilities of an organization in terms of identifying and responding to threats.
- **Coordination :** Essential for effectively pooling the response capabilities of various stakeholders and avoiding conflict
- **Capacity:** Encompasses the ability of an organization to implement and execute its security strategy effectively.
- **Cooperation :** Public-private partnership (PPP), including cooperation with industry partners, the financial sector, academia and law enforcement, plays an important role in increasing cyber security and resilience through raising awareness of threats, improving the overall intelligence picture, leveraging cyber security networks and preparing adequate support for an effective response.

An increased understanding of existing capabilities and accurate assessment of needs is required. This will provide greater awareness of risks and improve the security readiness process.



SECOND TECHNICAL SESSION

»» Theme: Best Practices in Cyber Security

Part - I

»» 1130 - 1200 Hrs: Sh. Vikas Tiwari, Head of Solution Architecture – India Central Government, Amazon Internet Services Pvt Ltd. (AWS)

»» Topic: Secure Cloud Services

The second technical session was held from 11:30 AM to 1:00 PM and was based on the theme “Best Practices in Cyber Security”.

Sh. Vikas Tiwari delivered his talk on the topic “Secure Cloud Services”. In his talk, he covered major points related to Cloud Security including, Approach to Cyber Security in Indian Context, Building your secure and compliant solutions in the Cloud, How AWS provides Zero Trust Security against the Internal and External Threats.

For many government departments moving to Cloud, the security model can be different from their traditional on-premise infrastructure. While the security requirements will likely remain constant, the security controls that meet these requirements may be different. Security teams often ask the following questions:

- Do I have adequate security to protect my workloads and data?
- How ‘good’ is good enough?
- What security controls do I need?
- Do I have validation that the right controls were built?
- Do I have verification that the controls work as planned?

He mentioned about the Data Breach incidences of 2019, which includes approx. 3800 publicly disclosed breaches, approx. 4.1 billion records exposed and 54% increase in data breaches. Further he mentioned about How privacy regulations are attempting to protect the consumers?

He then discussed the various standards of cybersecurity as follows:

- **Global Security Standards:** Cloud Security Alliance Controls (CSA), ISO 9001 Global Quality Standard, ISO 27001 Security Management Controls, ISO 27017 Cloud Specific Controls, ISO 27018 Personal Data Protection, PCI DSS Level 1 Payment Card Standards, SOC 1 Audit Controls Report, SOC 2 Security, Availability & Confidentiality Report, SOC 3 General Controls Report
- **United States Standards:** CJIS Criminal Justice Information Services, DoD SRG DoD Data Processing, FedRAMP Government Data Standards, FERPA Educational Privacy

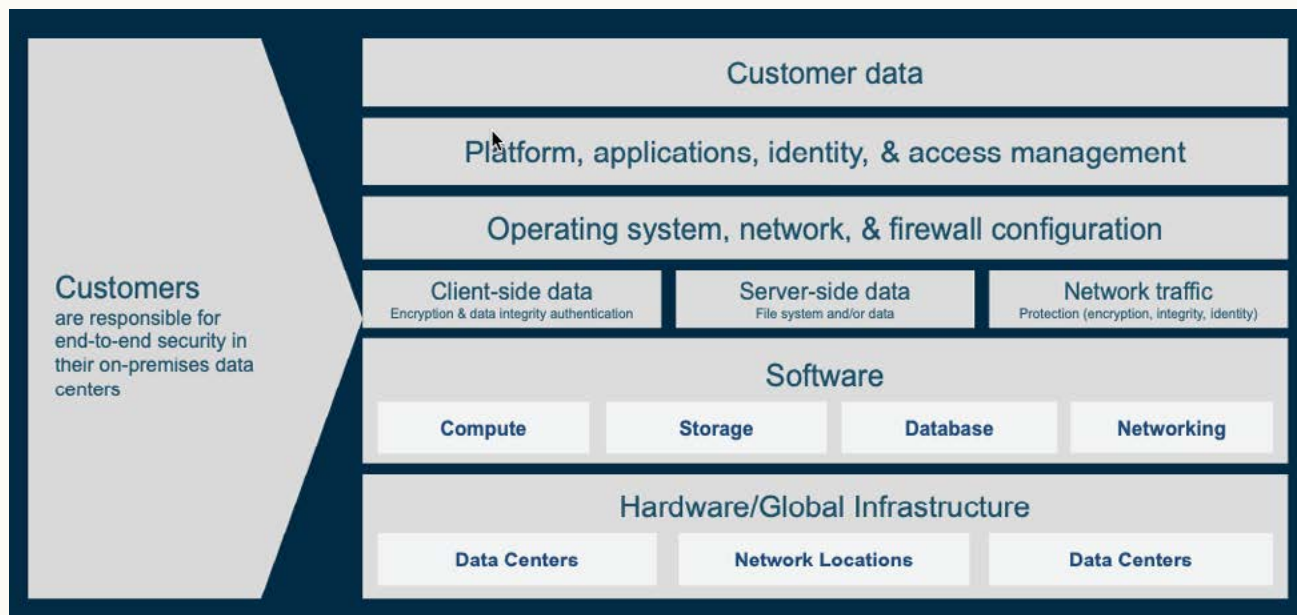
Act, ISO FFIEC Financial Institutions Regulation, FIPS Government Security Standards, FISMA Federal Information Security Management, GxP Quality Guidelines and Regulations, HIPAA Protected Health Information, CCPA California Consumer Privacy Act of 2018, ITAR International Arms Regulations, MPAA Protected Media Content, NIST National Institute of Standards and Technology, SEC Rule 17a-4(f) Financial Data Standards, VPAT/Section 508 Accountability Standards

- **Asia Pacific Standards:** FISC [Japan] Financial Industry Information Systems, IRAP [Australia] Australian Security Standards, K-ISMS [Korea] Korean Information Security, MTCS Tier 3 [Singapore] Multi-Tier Cloud Security Standard, My Number Act [Japan] Personal Information Protection
- **Europe Standards:** C5 [Germany] Operational Security Attestation, Cyber Essentials Plus [UK] Cyber Threat Protection, G-Cloud [UK] UK Government Standards, IT-Grundschutz [Germany] Baseline Protection Methodology, GDPR [EU] General Data Protection Regulation

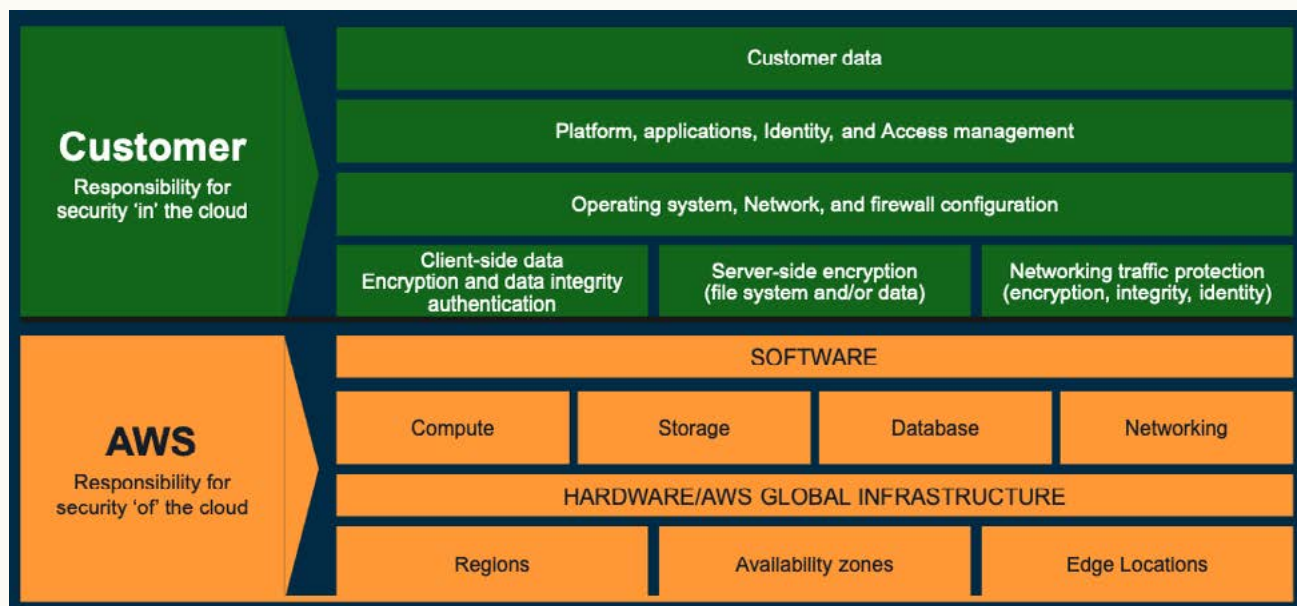
Global	United States	Asia Pacific	Europe
 CSA Cloud Security Alliance Controls	 CJIS Criminal Justice Information Services	 ITAR International Arms Regulations	 IDA MTCS Tier 3 [Singapore] Multi-Tier Cloud Security Standard
 ISO 9001 Global Quality Standard	 DoD SRG DoD Data Processing	 MPAA Protected Media Content	 My Number Act [Japan] Personal Information Protection
 ISO 27001 Security Management Controls	 FedRAMP Government Data Standards	 NIST National Institute of Standards and Technology	
 ISO 27017 Cloud Specific Controls	 FERPA Educational Privacy Act	 SEC Rule 17a-4(f) Financial Data Standards	 C5 [Germany] Operational Security Attestation
 ISO 27018 Personal Data Protection	 FFIEC Financial Institutions Regulation	 VPAT/Section 508 Accountability Standards	 Cyber Essentials Plus [UK] Cyber Threat Protection
 PCI DSS Level 1 Payment Card Standards	 FIPS Government Security Standards	 Asia Pacific	
 SOC 1 Audit Controls Report	 FISMA Federal Information Security Management	 FISC [Japan] Financial Industry Information Systems	 G-Cloud [UK] UK Government Standards
 SOC 2 Security, Availability & Confidentiality Report	 GxP Quality Guidelines and Regulations	 IRAP [Australia] Australian Security Standards	 IT-Grundschutz [Germany] Baseline Protection Methodology
 SOC 3 General Controls Report	 HIPAA Protected Health Information	 K-ISMS [Korea] Korean Information Security	 GDPR [EU] General Data Protection Regulation
	 CCPA California Consumer Privacy Act		

There are initiatives already taken by India for Cloud Security, including the MeitY Cloud Empanelment and the Personal Data Protection Bill.

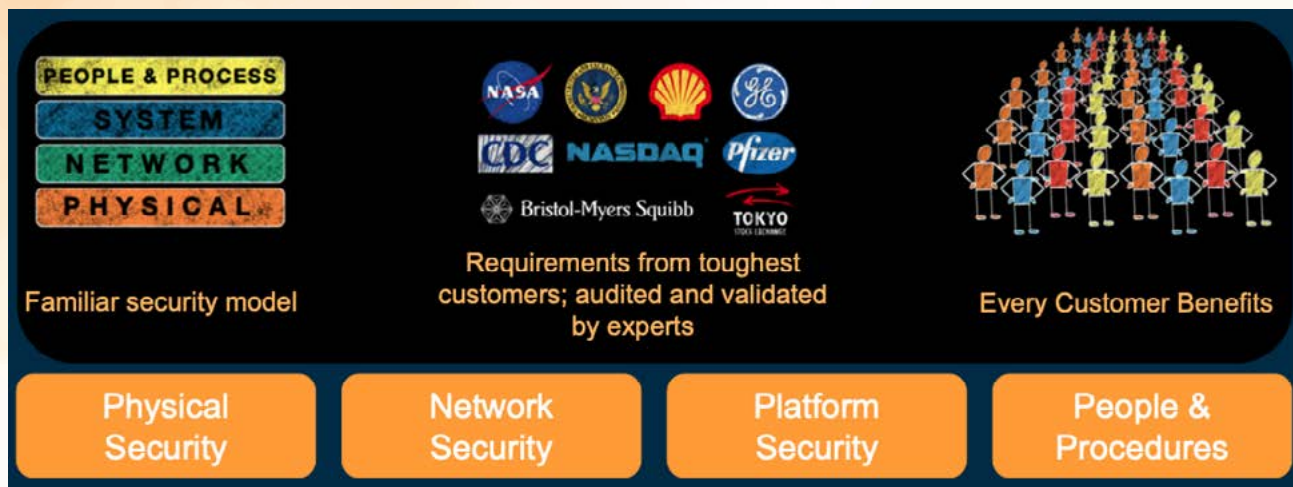
Sh. Vikas Tiwari also mentioned about the Traditional on-premises security model, as shown below:



He also mentioned that with AWS, Security and Compliance are a shared responsibility. Architecture of AWS is shown below:



According to him, this is how the Security is managed in AWS, as shown below:



The different sectors/stakeholders which use the AWS, including Government, Banks, Retail, Media, Healthcare etc., as shown below:



Metric observations monitored by Amazon Cloud Watch is 1 quadrillion plus. There are 230 Security, compliance, and governance services and key features. All the services support server-side encryption. It has 100% Compliance with the General Data Protection Regulation (GDPR).

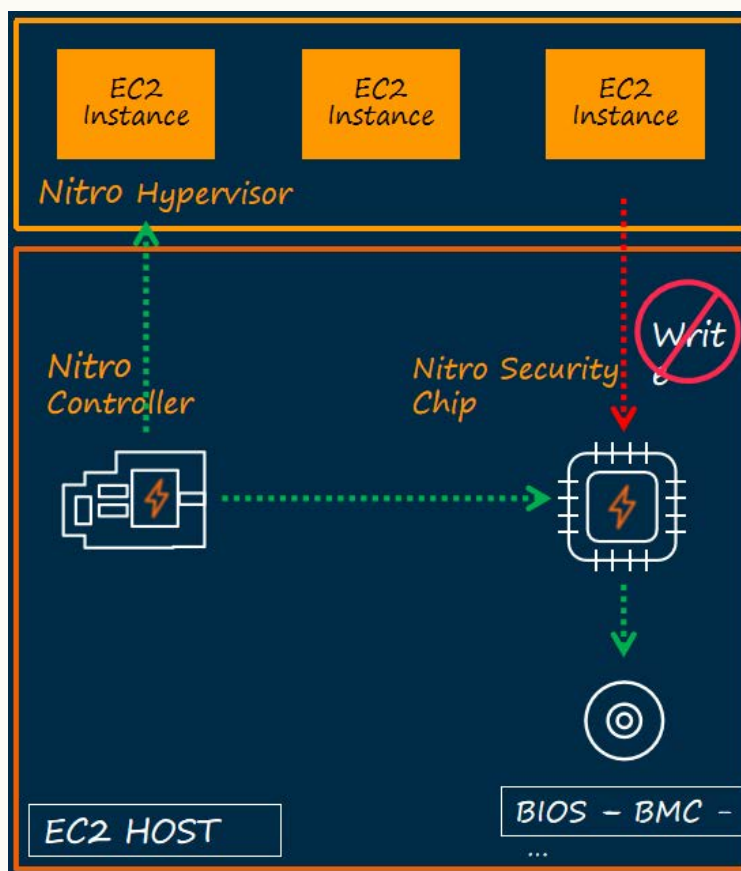
He discussed further about how AWS provides Zero Trust Security? There are various internal threats, which include Protection from Cloud operators, Protecting data from CSP software, Protecting sensitive data from Customer's own Administrators.

AWS Nitro system was also discussed along with the Modular building blocks for secure and rapid design and delivery of EC2 instances, as shown below:



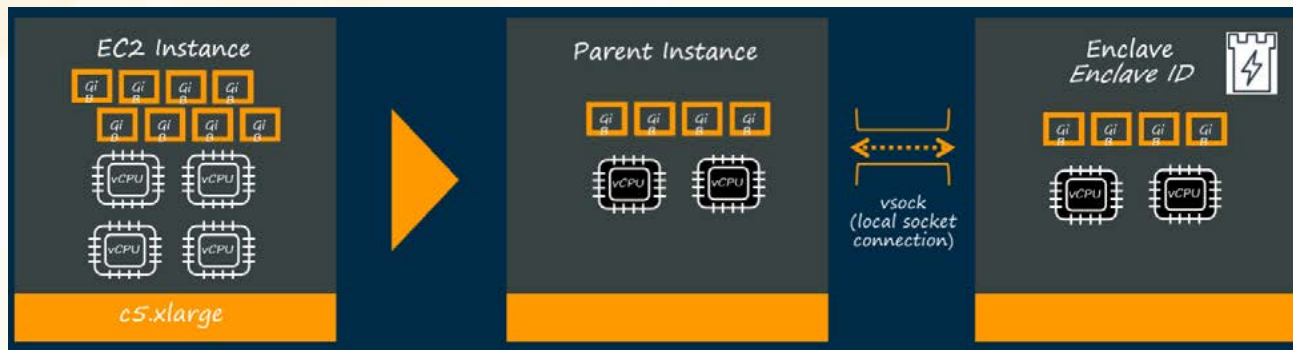
About the Nitro controller and Nitro Security Chip:

- Nitro Controller coordinates all other Nitro cards, the server hypervisor, and the Nitro Security Chip and implements H/W root of trust
- Nitro security chip blocks all write-access to non-volatile storage and implements the hardware root of trust
- Locked down security model prohibits all administrative access



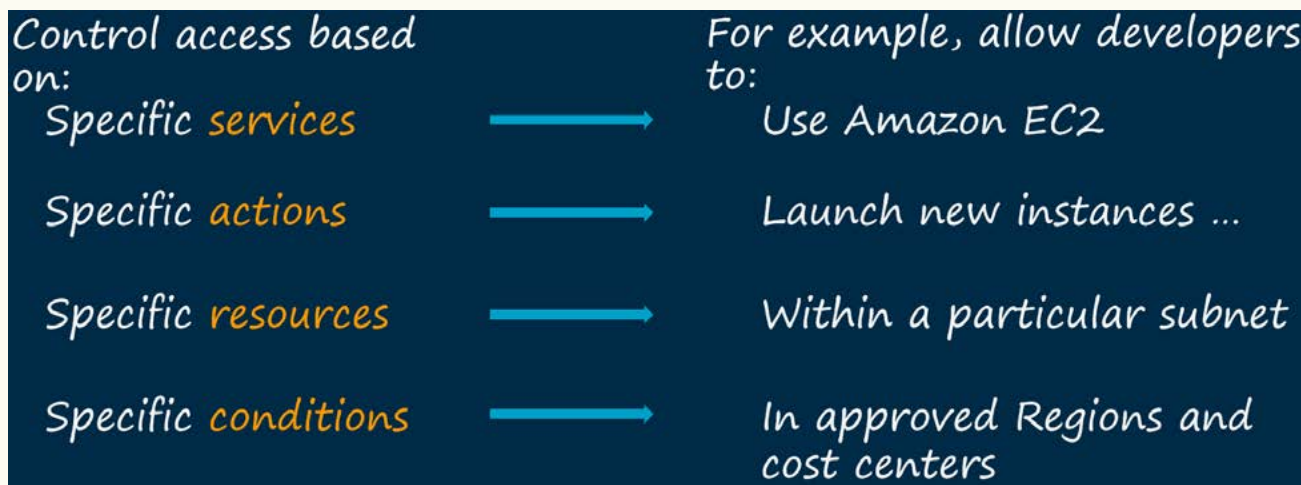
Further he mentioned about the AWS Nitro Enclaves – Confidential Computing, which includes:

- Partition the CPU and Memory of EC2 instance
- Resources are allocated to the enclave for the duration of its lifetime
- Enclave is active only while its parent instance is in the running state
- Single Enclave per parent

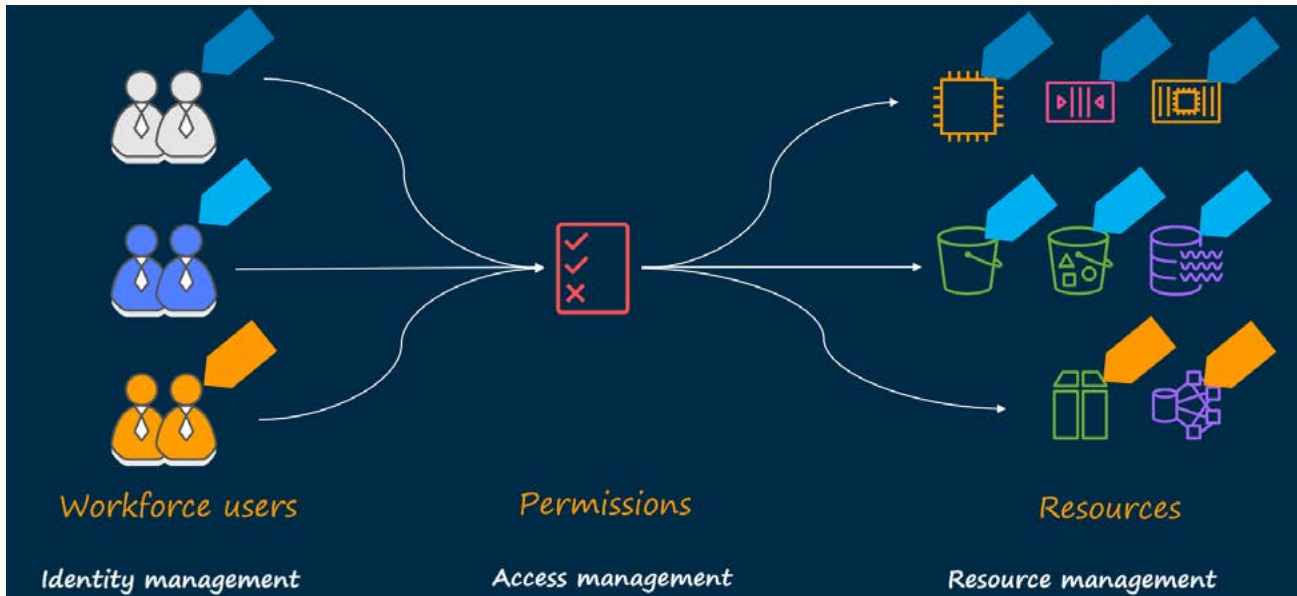


AWS also provides Zero Trust Security from the External Threats, including the Identity Controls and Network Controls.

AWS provides fine-grained access controls.



It also provides Attribute-based access control (ABAC), where, If the tag on the principal matches the tag on the resource, allow; otherwise, deny.



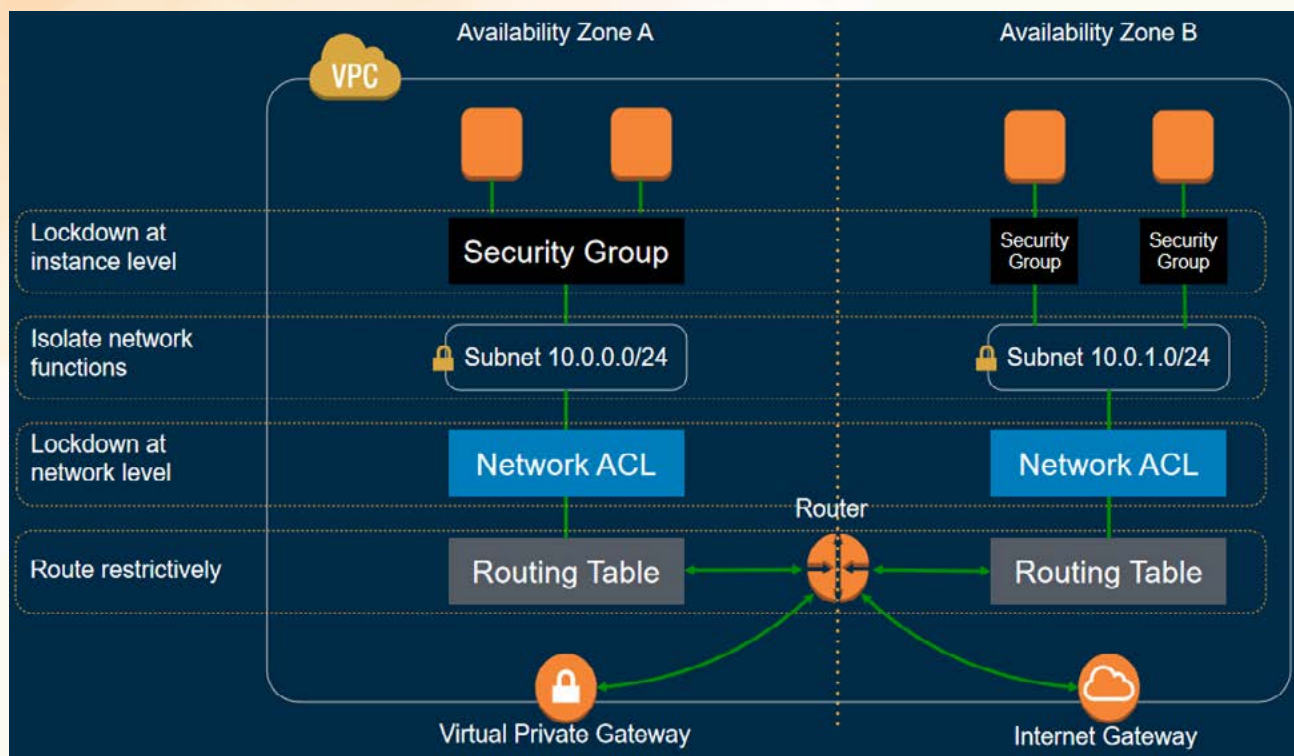
AWS provides Network Controls: AWS cryptography stack.



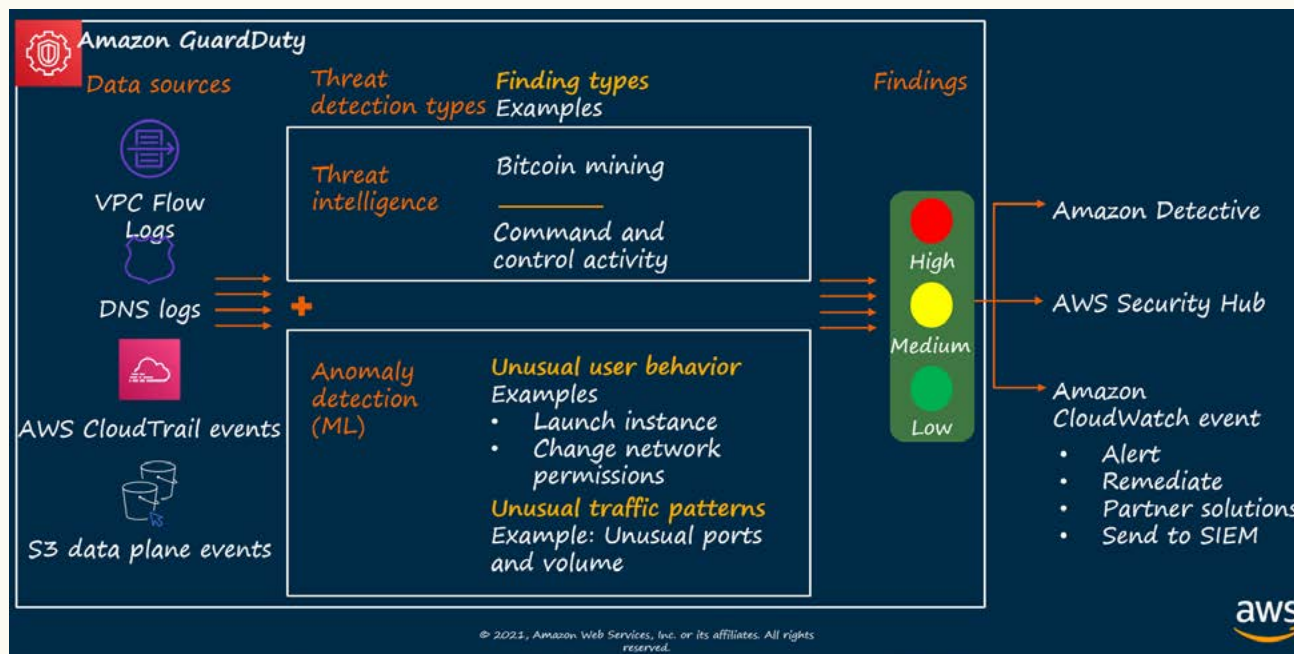
He explained about the process of Interacting with AWS Application Programming Interfaces (APIs) and how Zero trust within AWS

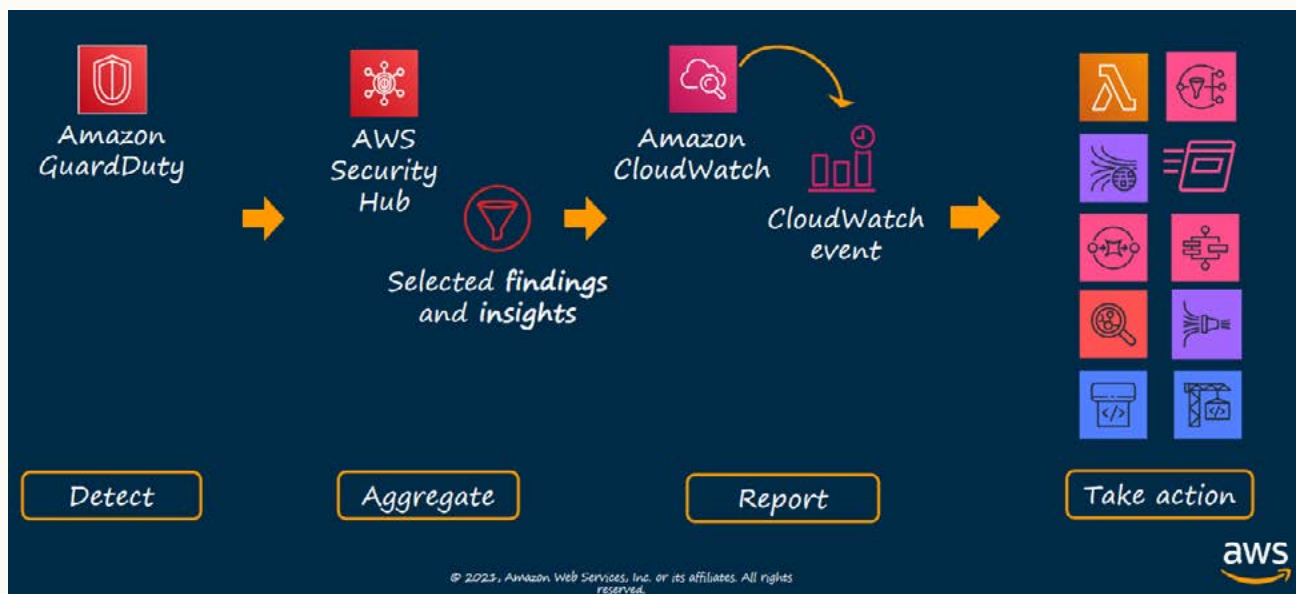
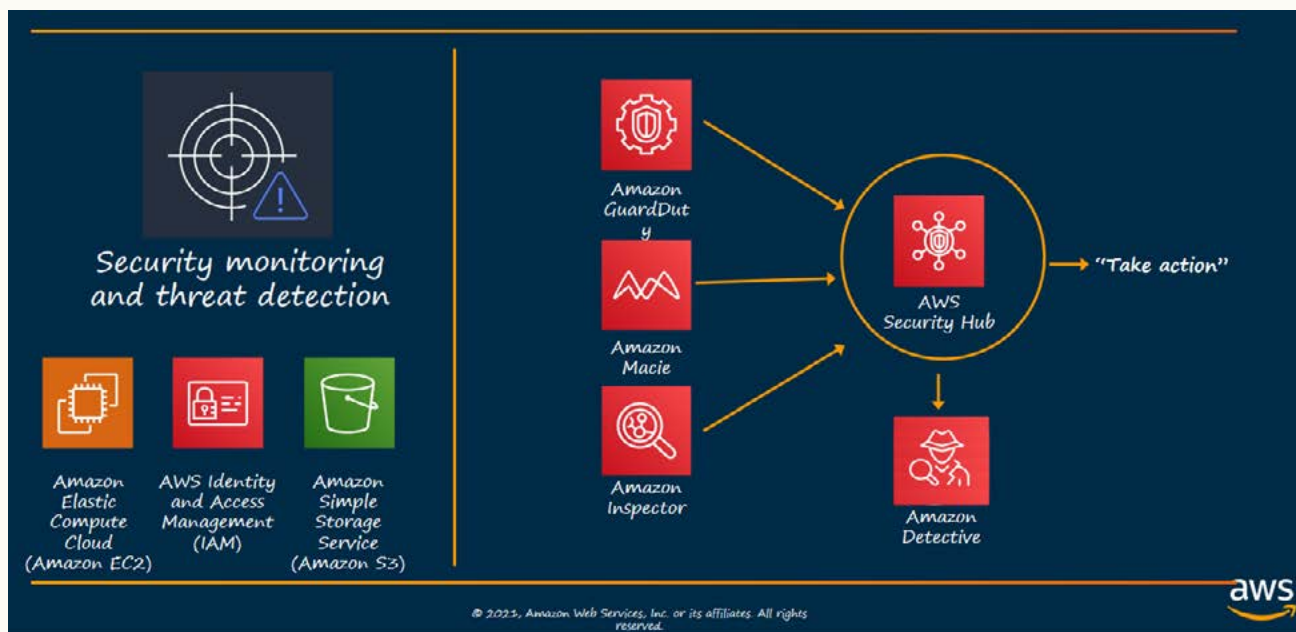


Security layers of Amazon Virtual Private Cloud (VPC) are explained with its architecture:

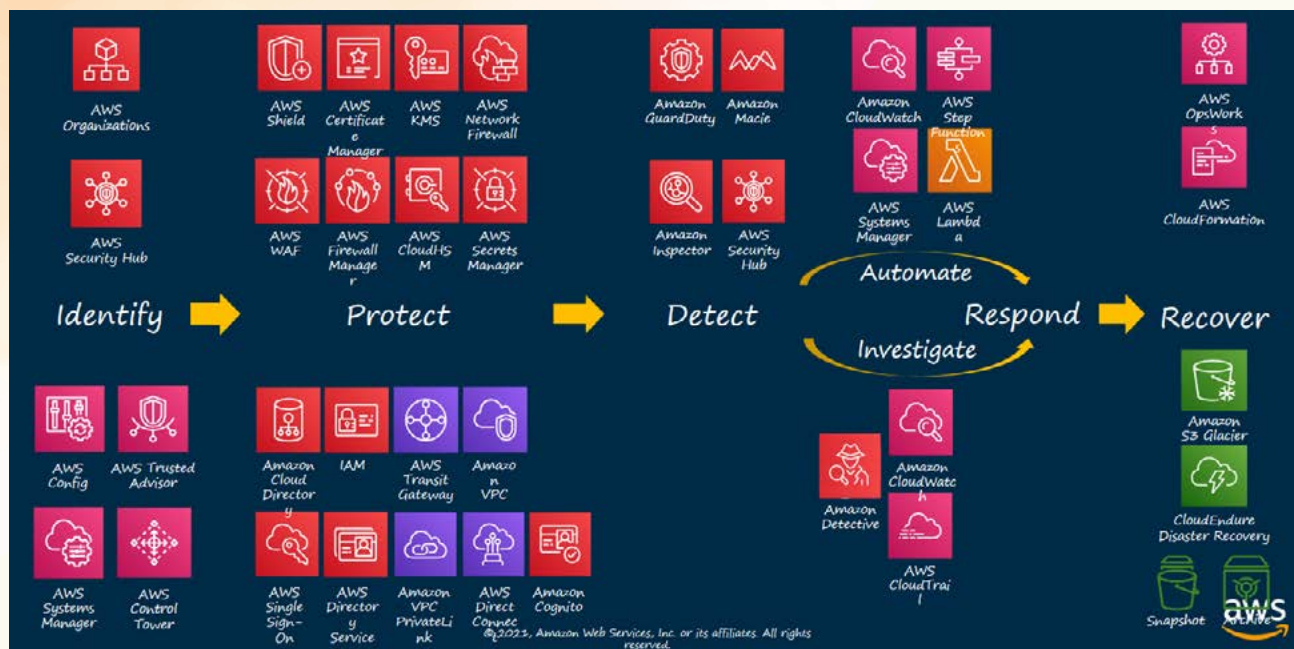


This is how for Threat Detection, the Machine Learning is used at scale, along with the Threat detection, monitoring, and response, as shown below:





Followings are the AWS foundational and layered security services:



Sh. Vikas Tiwari also mentioned about the AWS Services Alignment with the CSF. As validated by a third-party assessor, the services that maintain an accreditation under FedRAMP Moderate and/or ISO 27001/27101/27017 align with the CSF. It includes:

- Validated the NIST CSF Citations mapping to NIST SP 800-53 security control requirements
- Reviewed the AWS services that have undergone the FedRAMP Moderate and ISO 9001 / 27001 / 27017 / 27018 accreditations that meet the citation or control requirement
- During the service validation, identified additional citations that may have available scoped services that meet the requirement.
- All services recommended for inclusion were validated as in scope to the AWS FedRAMP Moderate and ISO attestations- marked with *italics* in workbook

When deploying AWS solutions, organizations can have the assurance that AWS services uphold risk management best practices defined in the CSF and can leverage these solutions for their own alignment to the CSF.



Part - II

» 1200 - 1230 Hrs: Sh. Vaidyanathan R Iyer, CISA CISM, COO,
IBM Security Command Asia-Pacific

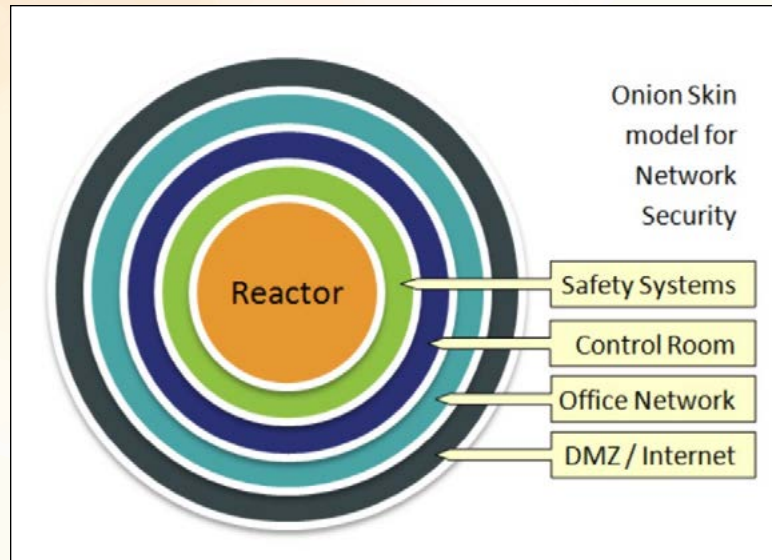
» Topic: Secure Network Infrastructure

Sh. Vaidyanathan R Iyer, delivered his talk on the topic “Secure Network Infrastructure”. In his talk, he briefly discussed his perspective about the Network as we knew and the Network of today.

He discussed today’s Threat Landscape, which includes Ransomware, Phishing, Identity theft, Social Engineering, OSINT etc. He also discussed the 2 major goals of Network Security i.e. Resilient and Defendable. There are 2 following focus areas:

- Control Systems
 - ✧ Static model/traditional defense systems
- Data Systems
 - ✧ Data residence and Data flow/dynamic risk assessment model

He also discussed about the Onion Skin model for CoreControl Systems:



As we all know, Data is the lifeblood of any entity. Network Protection is an enabler and the actual protection is to the data. The Common strategy to handle Data includes Data at rest, Data in motion, Data in Use, Data Access, Data Exfiltration.

For securing the Network by going beyond the Network, System Hardening, Application Hardening and moving network to data are the possible solutions.

System hardening can be done at:

- Operating System level
 - ⌘ Unix
 - ⌘ Windows
- End Point level
 - ⌘ Corporate End points
 - ⌘ BYOD

Application hardening can be done by:

- Use an Application Firewall
- Use secure protocols for applications
- Use automated vulnerability tools
 - ⌘ Test protocol- based vulnerabilities

The other solution which is moving perimeter close to the Data includes:

- Data Server Firewall
 - ⌘ Protect Web Server with WAF

⤴ Windows File server with Identity Aware Firewall

Identity is very important as a function of network security as, while connecting to the corporate Wi-Fi, user identity and device identity are very essential. For a corporate server, the user identity, organizational identity and device identity are essential.

He further discussed the Anomaly detection in today's networks by analyzing the Networks logs, Endpoint logs and Appliance logs, Link logging to Analytics and Security Intelligence, Using correlation analysis across sources and Big Data Analytics usage.

There are various High Security Networks including:

- Financial Trade
- Secure Labs (Scientific research Labs)
 - ⤴ Only trusted device can be allowed
 - ⤴ Use Port-based Network Access Control
- Leverage Identity & Encryption
 - ⤴ Go beyond generic firewalls
 - ⤴ User behavior Analysis

Sh. Vaidyanathan R Iyer then concluded his talk by sharing the best practices in Secure Network Infrastructure as follows:

- Outside Insecure, Inside Secure model is obsolete
- Data flow analysis drives network security in the era of DX
- Network security should function with secure identity posture
- Continuous risk assessment is the key
 - ⤴ Maintain an Asset Register (update periodically)
 - ⤴ Segregate OT assets from IT Assets
 - ⤴ Implement protection & Detection capabilities

Part - III

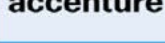
» 1230 - 1300 Hrs: Sh. Shrikant Shitole, FireEye

» Topic: Challenges in Prevention and Mitigation of Cyber Threat

Sh. Shrikant Shitole, in his talk briefly discussed “Challenges in Prevention and Mitigation of Cyber Threat”. As we know, Data Breaches & Hacks are getting more and bigger by the day.

He discussed the following instances of Data Breaches & Hacks.

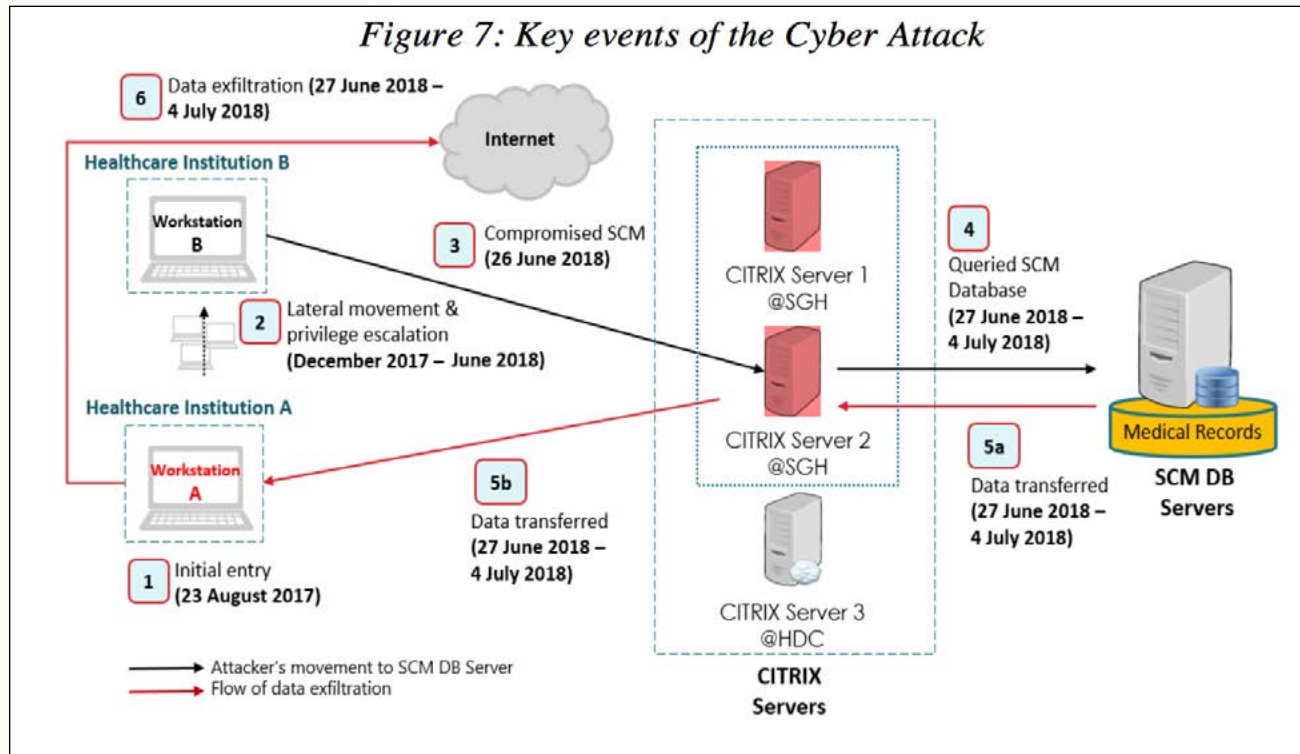
Company	Threat Actor(s)	Motivation(s)	Methods	Impact	Remarks
	Nation State	Espionage	Not disclosed	Access to 18000+ companies	Suspect APT29?
	Nation State	Espionage	Solarwinds, MS Zero Day	Red Team Tool, Solarwinds breach uncovered	Sunburst !!
	Cyber Criminals	Financial, Supply Chain Access	0-Day Exploits, Webshell	Access to 100+ companies	FIN11, Clop
	Cyber Criminals	Financial	Unknown	30M asked, data	REvil
	Nation State?	Supply Chain Access	Unknown	30K+ customers affected	Microsoft attribute to China
	Cyber Criminals	Financial	Accellion 0-Day	Customers, data	Clop
	Cyber Criminals	Financial	MS Exchange 0-Day?	50M asked, data	REvil
	Nation State	Supply Chain Access	Not disclosed	Access to many customers	

Company	Threat Actor(s)	Motivation(s)	Methods	Impact	Remarks
	Cyber Criminals	Financial	Not disclosed	50M asked, Apple product new design	REvil
	Cyber Criminals	Financial	Compromised password in darkweb	4.4M paid, disruption	Darkside
	Cyber Criminals	Financial	Not disclosed	Ransom, data	Avaddon
	Cyber Criminals	Financial	Not disclosed	11M paid, disruption	REvil
	Cyber Criminals	Financial, Supply Chain Access	Not disclosed	70M asked, Access to many customers	REvil
	Cyber Criminals	Financial	Accellion 0-Day used by supplier	Data	
	Cyber Criminals	Financial	Not disclosed	Data	LockBit

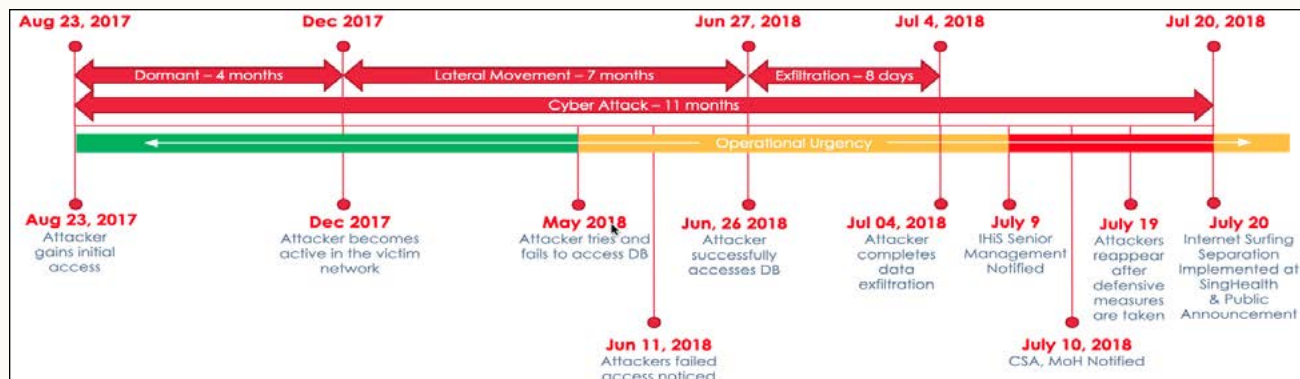
Further he discussed the anatomy of an attack on Singapore Health Services. The SingHealth Sunrise Clinical Manager (SCM) system was identified as a CII system within the healthcare sector in 2011, and also as a mission-critical system for SingHealth. There are 11 Sectors of Critical Information Infrastructures: Government, Infocom, Energy, Aviation, Maritime, Land transport, Healthcare,

Banking & Finance, Water, Security and Emergency, Media etc.

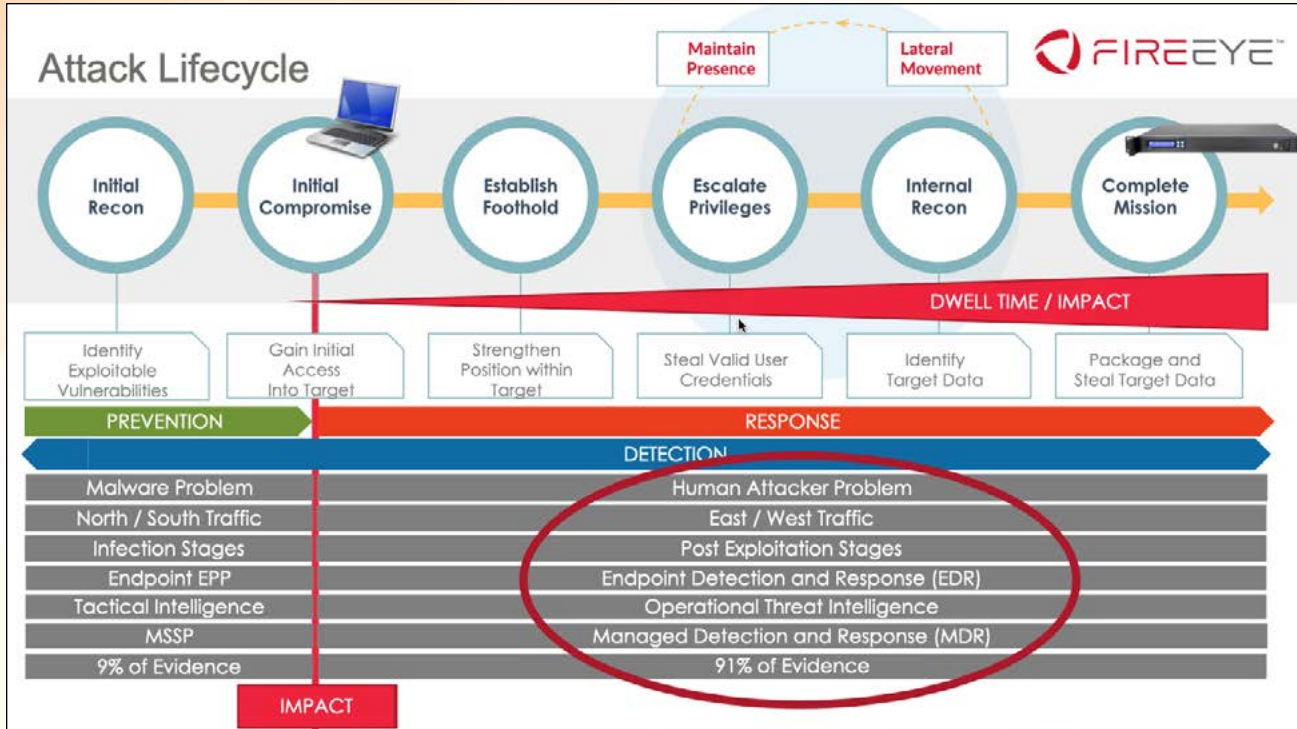
Further he discussed about the Attack Life Cycle and Key events of the Cyber Attack:



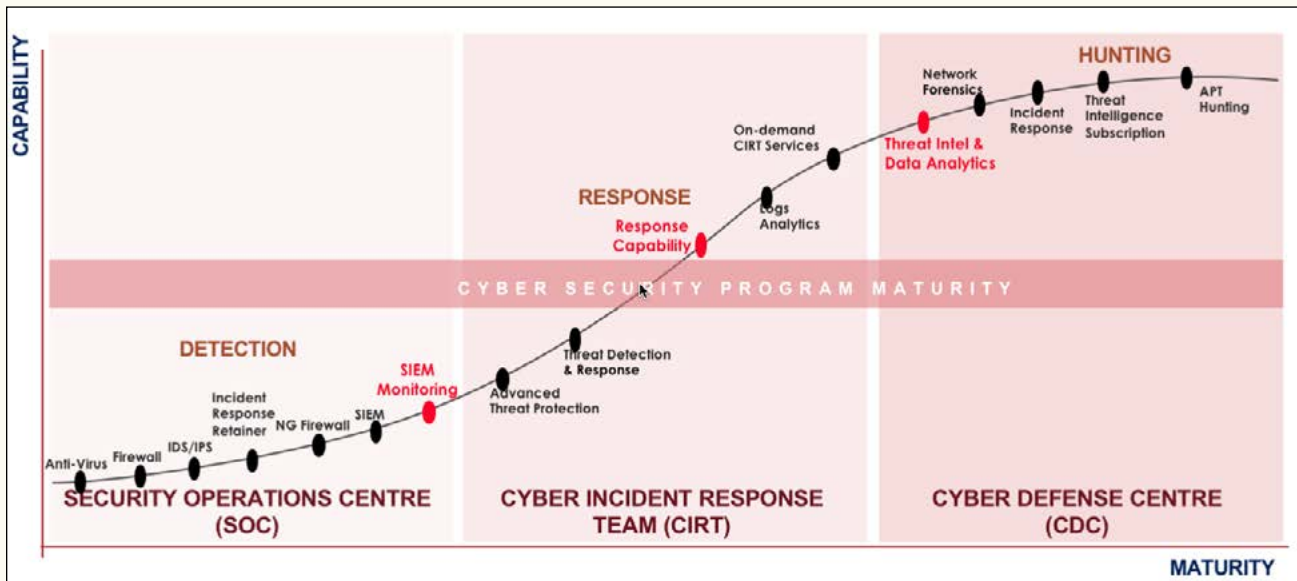
He also discussed about the Attack Timeline with an example scenario:



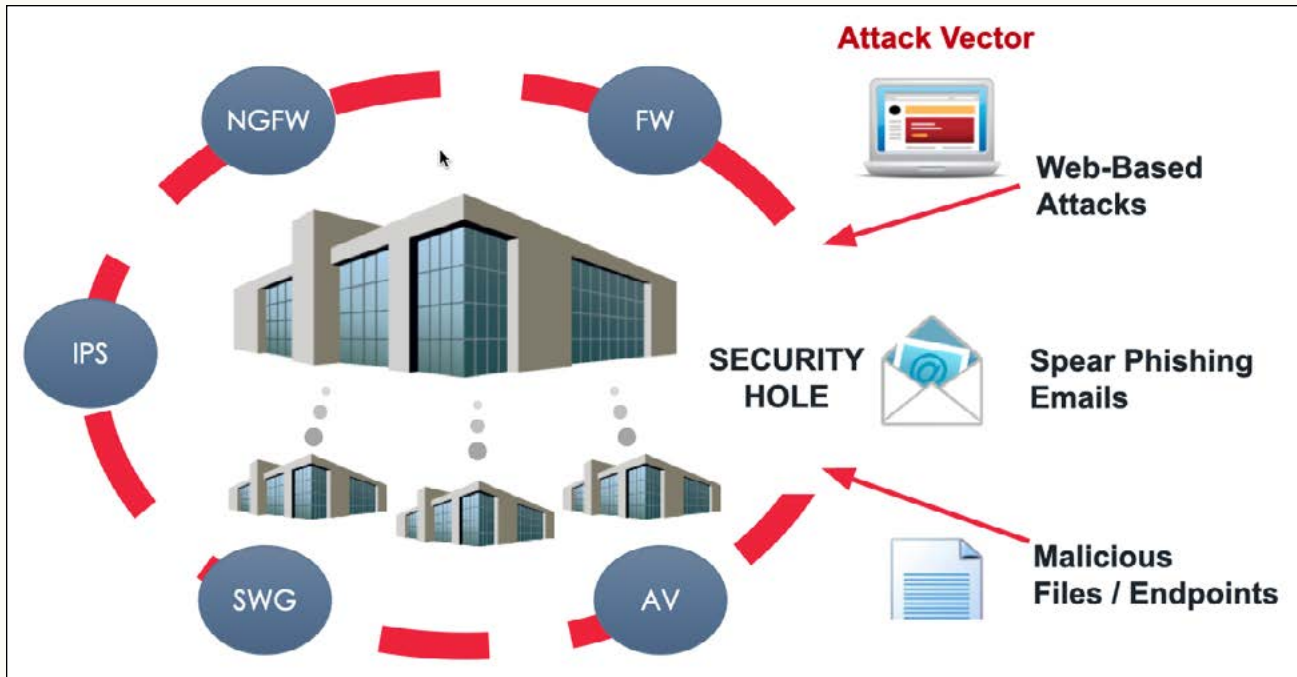
He discussed about the Attack Life Cycle in terms of Detection, Response and Prevention, as follows:



Cyber Security Maturity Curve has been discussed in detail with more focus on Prevention (i.e. Malware), Detection & Response (i.e. Human Attackers)



Enterprise Security has multiple Attack Vectors including:



Here is the checklist for ensuring whether the organization is ready to respond to cyber security incidents?

- Do high level simulation, e.g. Table Top Exercise for management and technical team
- Do Red Team exercise to assess readiness of security control, people and process
- Consider automated validation mechanisms
- Use the gap analysis from the exercises to prioritize investment

Here is the action plan one may follow in case of encountering a ransomware:

- Backup your files
- Educate end users
- Patch vulnerabilities
- Employ advanced email threat detection
- Use a good EDR solution
- Focus on both N-S and E-W traffic
- Provide the least amount of privilege possible
- Logically separate networks
- Implement good best practices for solution that you use



Following are the suggestions for how quickly the team can respond to cyberattacks? (eg: phishing, ransomware, etc)

- Make sure you have technology that can detect and protect
- Focus On Both Defense AND Resilience
- Educate the people – Management & Operations
- Design your playbooks, test and revise it
- Include Managed Detection & Response services from reputable vendor if you can't staff 24x7 for all level of analysts
- Review your process to include a retainer and how an external expert can step in to help

By sharing the insights and best practices for Prevention and Mitigation of Cyber Threat, Sh. Shrikant Shitole concluded his talk.

THIRD TECHNICAL SESSION

Theme: Securing Critical Cyber Physical Infrastructure

Part - I

»» 1400 - 14:10 Hrs: **Sh. Rinka Singh, iSprit**

»» **Topic: Secure Online Public/Financial services and Citizens' Data**

The third technical session was held from 2:00 PM to 2:10 PM and was based on the theme “Securing Critical Cyber Physical Infrastructure”.

Sh. Rinka Singh, core volunteer iSprit– delivered his talk on the topic “Securing Public and Citizens Data”.

In his talk, he covered points related to best practices for data security and system security and application within iSprit. He also mentioned the importance of management of the data, information, software and apps. He addressed that, we don't have a data management system so, the technological innovations here for learning from our mistakes and doing it the perfect way. He added that we need a clear exploration and thinking styles in a comprehensive way. He has also talked about the project Sakram. It is mainly for cyber secure society. They are currently working on the airlines and hospital industry effectively. This project is converting our experiences into questions and checklists. Then, it can be automated and deployed. This software eventually covers a wide area of the population.

The conclusion of the talk remains that “leveraging the community”.

Part - II

»» 1410 - 14:30 Hrs: **Mr. Pronab Mohanty, IPS. Deputy Director General, Unique Identification of India.**

»» **Topic: Secure online public financial services and citizen data.**

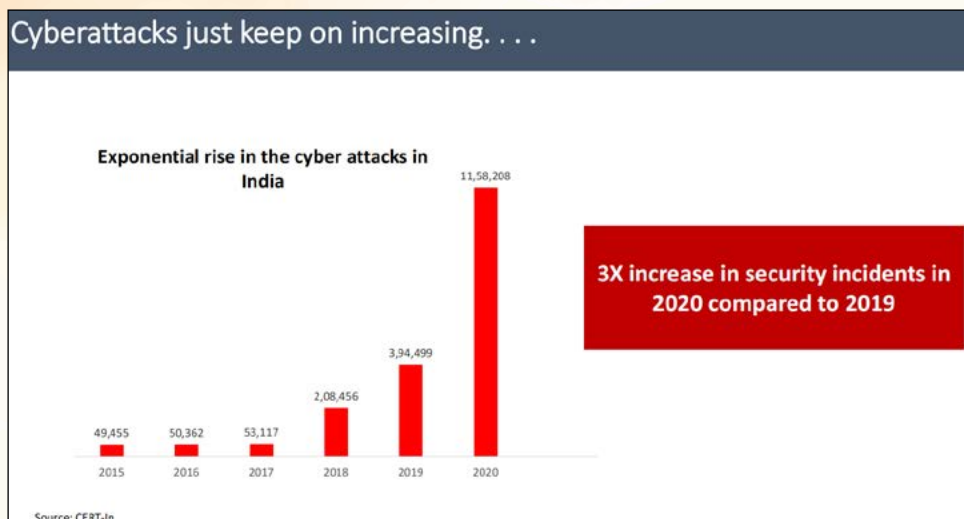
The third technical session part 2 was held from 2:10 PM to 2:35 PM and was based on the theme “Secure online public financial services and citizen data”.

Mr. Pronab Mohanty, Deputy Director General, Unique Identification of India– delivered his talk on the topic “changing cyber security landscape and evolving role of CISOs”.

He addressed two topics;

- how the cyber landscape is changing

- how the roles of CISOs are evolving along with it.

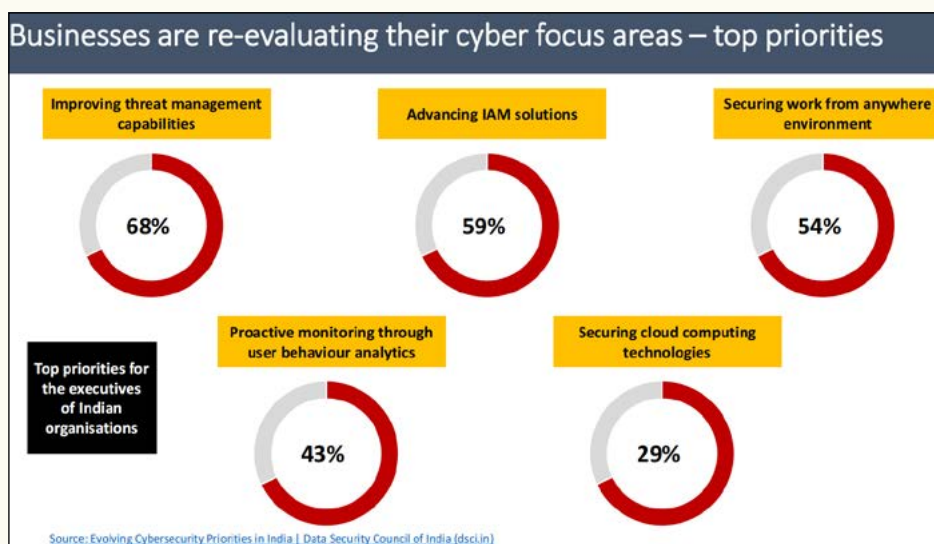


He discussed further about the rate of cyber attacks in India. There was an exponential rise in security incidents in 2020 compared to 2019.

It was noted, we can assure that there will be many more cyber attacks in 2021.

He discussed how different kinds of security measures are enough to tackle these novel types of cyber attacks. He addressed many questions related to data authentication and security mechanisms, followed by brief discussion on remote working, cyber resilience, supply chains, rapid digital adoption, cyber security priorities and unnecessary and large volume of data. He linked all of these ideas with a pandemic background.

After that he talked about businesses re-evaluating their cyber focus areas and he mentioned some of their top priorities.



Then, he spoke about the key areas of focus, it was mainly existing IAM solutions, security awareness and culture, advanced data and behaviour analytics, security maturity and others are prioritising secure cloud adoption.

Later he mentioned the role of CISOs in organisations. There, he discussed different types of CISOs.

- transformational CISO
- post-breach CISO
- tactical/operational expert CISO
- compliance and risk guru
- steady-state CISO
- customer facing evangelist

After discussing types of CISOs he moved into how the role of CISOs has changed over a period of time. There he spoke about how they reached to align security strategy with business strategy and how it will handle large and complex security technologies in future.

He mentioned what CISOs can do in their organization. He quoted that CISOs should influence the actions taken by C-suite keeping security in mind, aligning cyber objectives with business prerogative, build security and privacy, rapid digital transformation and custodian of customer data.

In a nutshell of CISOs he concluded his speech.





Part - III

»» 1430 - 15:00 Hrs: Balsing Rajput, DCP of crime branch Mumbai

»» Topic: “New perspective in cyber security for LEAs”

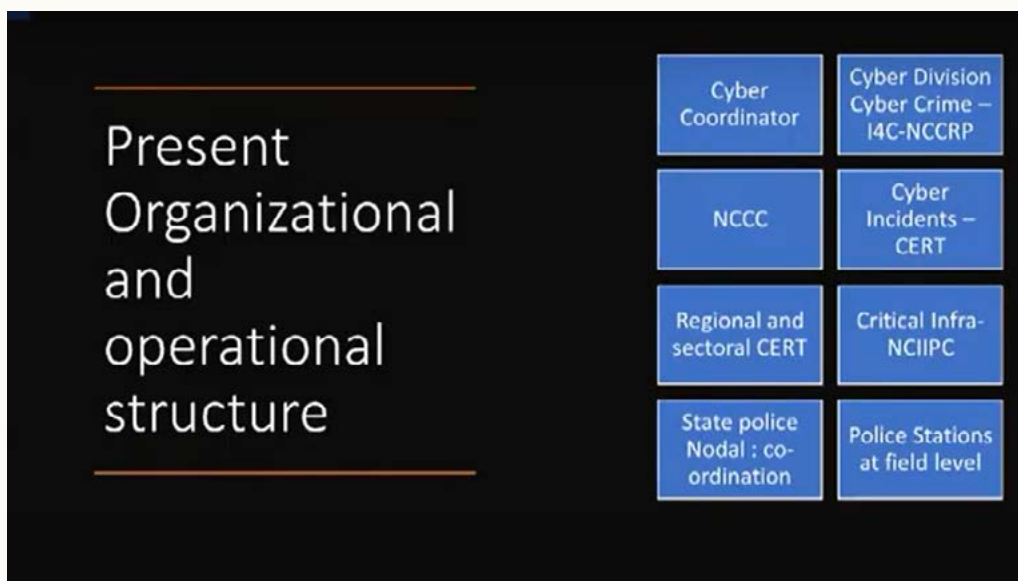
The third technical session part 3 was held from 2:30 PM to 3:00 PM and was based on the theme “Securing Critical Cyber Physical Infrastructure”.

Mr. Balsing Rajput, DCP of crime branch Mumbai, – delivered his talk on the topic “new perspective in cyber security for LEAs”.

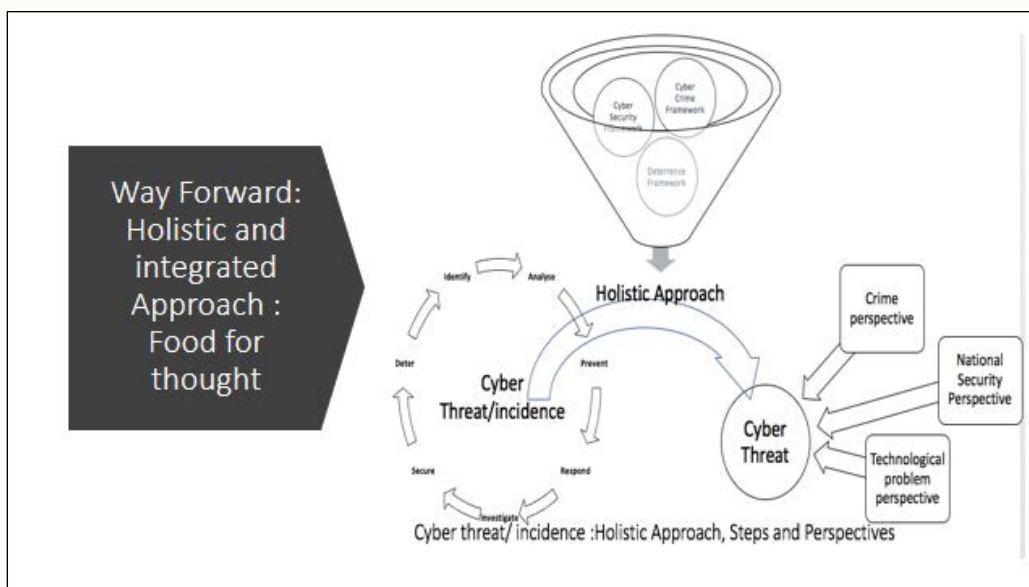
He delivered a speech on law enforcement and its focus. He stated that law enforcement mainly focuses more into causes and corrective actions. Later he spoke about perspectives of security and law enforcement agencies. He gave a clear picture about cyber attacks and their modus operandi. He mentioned changed technology scenarios in a broader perspective. There he talked about,

- cloud system
- IOT
- AI and ML
- mobile technologies
- OTT and online platforms
- Encryption in communications

Then he mentioned that ultimately all these technologies are used by perpetrators to commit crime. Later, he addressed the cyber security emerging threat landscape. He gave a detailed note about crimes, security cyber espionage, data theft and harvesting and law and order. He discussed LEAs daily fight for maintaining security and challenges of law enforcement agencies. Later he talked about how the technology world is marching towards integration, putting everything on a common platform, everything in place, every data is churned, decisions are data driven and AI and ML are behind that. He pointed out that institutional and organizational issues addressed related coherent and coordinated responses. He mentioned the present organizational and operational structure.



He stated that during his Ph.D, he did research on what will be an approach to deal with the cyber attacks.



He addressed that, for a way forward we need a policy framework, sharing information with LEA, and stolen or fake credentials. He concluded his talk with issues faced by law enforcement agencies.

Part - IV

» 15:00 to 15:15 Hrs: Mr. Venkatesh. S, Assistant Director, IB

» Topic: Cyber physical security and law enforcement agencies

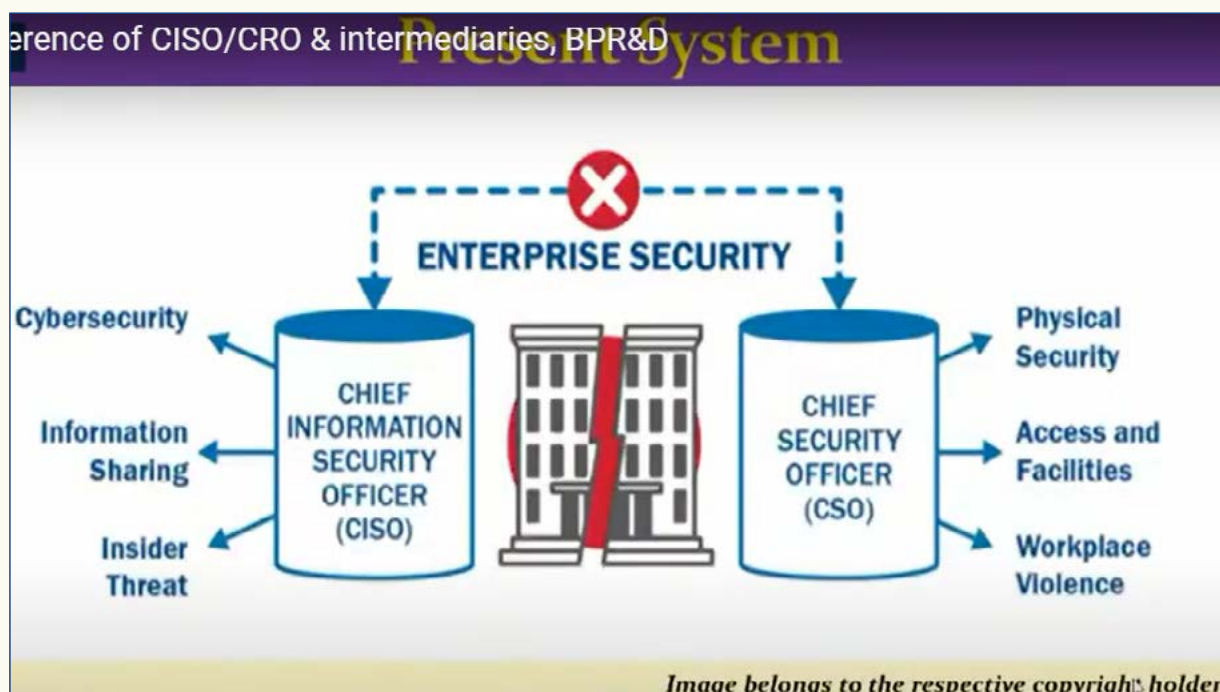
The third technical session part 4 was held from 3:00 PM to 3:15 PM and was based on the theme “Securing Critical Cyber Physical Infrastructure”.

Mr. Venkatesh. S, Assistant director IB, – delivered his talk on the topic “Cyber physical security and law enforcement agencies”.

He mentioned law enforcement agencies and their perspectives. Then, cyber physical systems were explained through the example of charlie chaplines movie called city of lights. He talked about cyber security challenges,

- threats
- critical
- infrastructural

He gave examples from health systems, pacemakers with wifi connectivity for real time data transmission to cardiologists. These pacemakers can be used to kill people with electric shock. Also, he mentioned hackers send spam emails using a web connected refrigerator. Later, he addressed day to day policing challenges. Also, for a way forward, we need cyber security as a shared responsibility, cyber threat intelligence sharing and cyber centre of excellence partnership. He spoke about the background of LEAs and organisation.



We need a convergent security system for CPS. That is,



He mentioned end users adopted SURAKSHA for safe internet access. He concluded that as a nation we need to develop a cyber security culture and maintain cyber hygiene in our day-to-day cyber life.

FOURTH TECHNICAL SESSION

»» Theme: Emerging Trends in Cyber Security

Part - I

»» 15:00 - 15:15 Hrs: Dr. Manan Suri, IIT - Delhi

»» Topic: Zero Trust Model of Security

The fourth technical session part 1 was held from 3:00 pm to 3:15 pm and was based on the theme “Zero Trust Model of Security: Importance of Hardware.”

Dr. Manan Suri, Associate Professor, IIT Delhi and Principal Investigator in NVM and Neuromorphic Hardware Research Group delivered his talk on the topic “Zero Trust Model of Security: Importance of Hardware.”

Dr. Suri focused on what he believed is one of the most important aspects that would help to translate zero trust security, is hardware. The term zero trust security was coined in 2010 by an analyst at Forrester Research Inc.



Underlying Key Principles of Zero Trust Security are:

- Trust no one and nothing
- There is no trust zone
- There is no safe zone

- Identity is instantaneous, i.e, there is no notion of time with identity in terms of network, premises. If an identity is being associated with any individual/entity, it needs to be re-evaluated time and again.

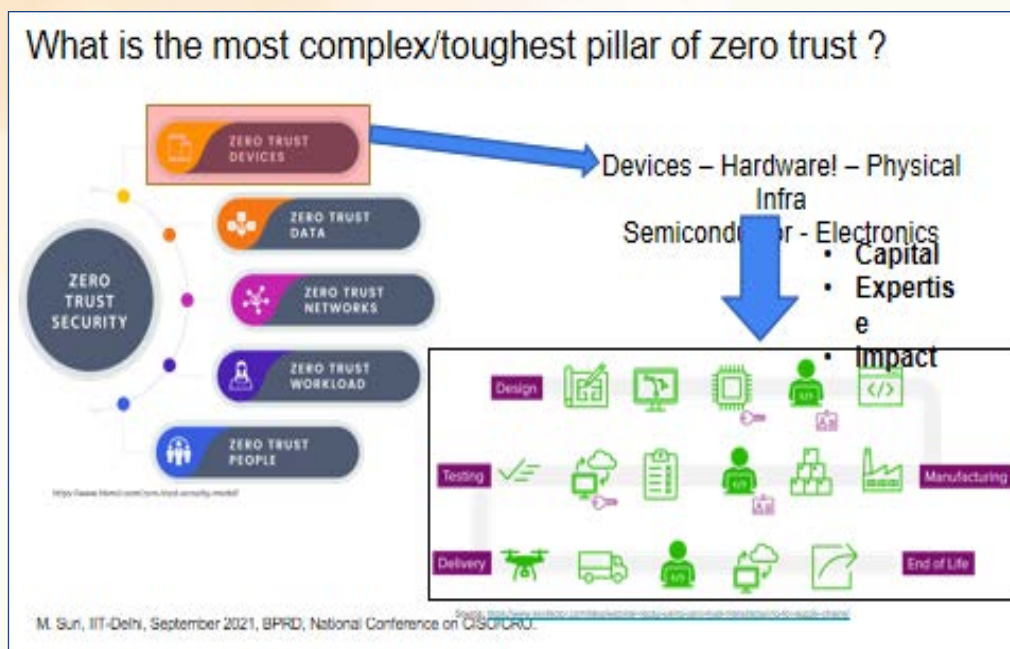
Five pillars on which the entire zero trust model is based on, are:

- Zero Trust Devices
- Zero Trust Data
- Zero Trust Networks
- Zero Trust Workload
- Zero Trust People

On these pillars one starts to build the zero trust model. Pillars consisting of devices, networks and people come under more traditional threat vectors which are considered while building any security system or protective environment. Whereas, pillars of data and workloads are new and emerging which would require a lot of precedence in the time to come. These are very futuristic. The concern regarding security in the past was limited to assessing whether the data contained any malicious code inside or whether it was infected by any virus. Dr. Suri further talked about current concerns of security where the data is contaminated intentionally to disrupt the AI algorithms or the NN paradigms that are supposed to be built in future. This is a challenging task because it's extremely difficult to catch unless some models are seen with their impacts. Workload is another interesting aspect because so many applications run in the background that does not support the conducive physical environment. As the nature of applications is becoming more computational, it becomes difficult to differentiate whether the resources are present because of the nature of the application or for intentional harm to the device/systems. These are the futuristic threat vectors that could pose challenges and need attention.

Principles of Zero Trust Security:

- Trust No one
- Least privilege access model
- Segment the Network
- Use Multi-factor authentication
- Device access control
- Inspect and log everything
- Be ready for a breach



The toughest/most complex pillar that makes or breaks the zero trust security is the ‘devices’ and specifically the hardware. The physical infrastructure, electronics, semiconductors on which all application and data remains. Hardware is a component that will ensure whether we have full proof zero trust security or not. These components are complex in nature and their working is different from that of applications. They have detailed design stages, testing stages and work in multiple layers and extensive and elaborate delivery stages.

Challenges while ensuring security at the hardware level:

- Capital
- Expertise
- Impact

Another Geopolitical threat is the supply chain of semiconductors as this is from where the hardware parts are being supplied. There have been a lot of cases where intentional contaminations has been done deeply inside the hardwares. There are so many open ends in a typical supply chain where intentional contamination can take place before the system is deployed in your hands. Some cases in open literature which talk about contamination or vulnerabilities are one of Bloomberg- in which malicious chips on Motherboard are inserted during manufacturing. During its entire manufacturing it moves to one continent for chip design, for fabrication it moves to another continent or country, and then finally get in our hands deployed in our system. So in the supply chain there are many open end points where intentional or unintentional security issues can crop up. This is something very serious. Therefore for true zero trust, the global chain has to be broken, which calls for local capacity/ability for ensuring true zero trust security.

Hardware Layer Threats to Zero Trust Model

In future, more threats will be deeply embedded in the hardware and it will be warfare of molecules and atoms literally and also figuratively. One of the famous case studies is from Intel and a lot of emphasis is given to hardware and specialized silicon hardware to build trust from the root.

On-Going Hardware Security Research instances at IIT Delhi were also enumerated.

- Semiconductor PUFs (physically unclonable functions)
- Hardware RNGs/PRNGs/Key Seeds
- Accelerated Crypto Engines
- Storage security- Forensics, recovery and defence
- Vulnerability assessment- Side channel/fault injection attacks

Conclusion

- Zero trust is a digital lifestyle-highly paranoid.
- There will be trade offs on performance due to additional verification overhead.
- Without focus on Hardware-zero trust is an illusion.
- In the time to come cyber physical security will be dominated by hardware considerations.

Part - II

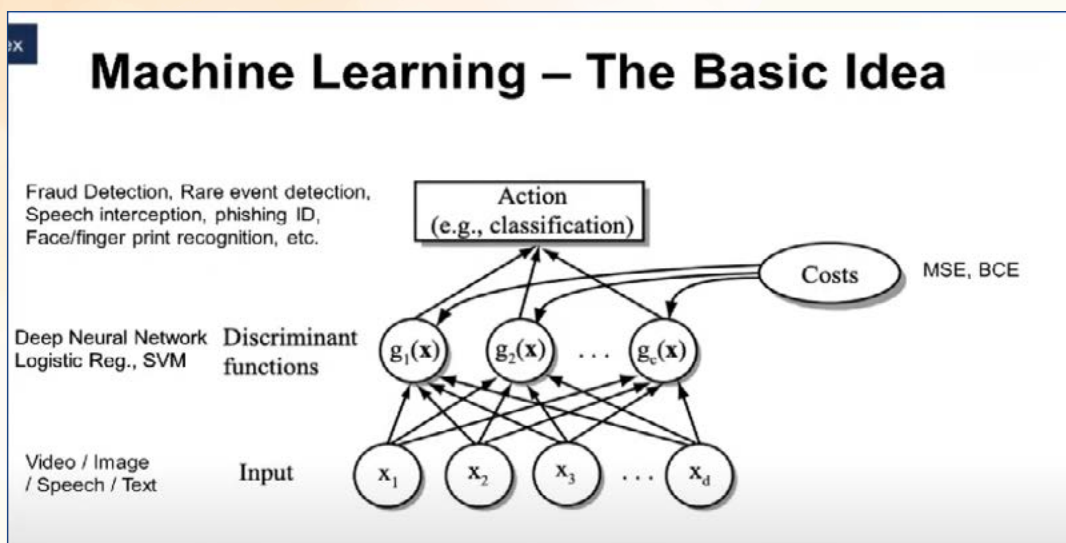
»» 15:15 - 15:30 Hrs: Dr. Prathosh A.P., IIT - Delhi

»» Topic: AI/ML for Security

The fourth technical session part 2 was held from 3:15 pm to 3:30 pm and was based on the theme “AI/ML for Security: Strengths, Challenges and Possible Remedies.”

Dr. Prathosh, Assistant Professor, IIT Delhi delivered his talk on the topic “AI/ML for Security: Strengths, Challenges and Possible Remedies.”

He started his talk by providing basic knowledge about machine learning.



Modern Machine Learning Strengths:

- Highly effective (surpass human performance) when provided with sufficient labelled data
- Matured models and techniques for diverse set of tasks
- Video analytics, speech processing, image/scene understanding, Natural Language Processing (NMT)
- Reduces manual efforts in handling mundane tasks (eg: scanning through CCTV footages)
- Can handle/process high volumes of data with ease
- Existence of pre-trained models on large databases

Issues with Machine Learning:

- Unavailability of large scale annotated data (need for expert annotators)
- Domain shift and strong inductive biases: for example- making a face recognition system for the US and deploying it for the Indian population. It will fail. So whenever there is a mismatch between training and the test condition, one should not trust it.

Domain Shift / Out of Distribution

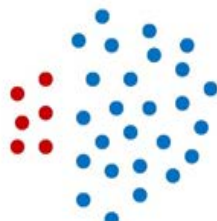


Figure: Examples from PACS, VLCS and Office-Home datasets.

- ML models do not know what they don't know (first step of intelligence)
- Models trained on one dataset does not work on the others (with different conditions)
- Speech recognition trained on American English doesn't generalize on Indian English

The Problem of Class Imbalance

Imbalanced Class Distribution

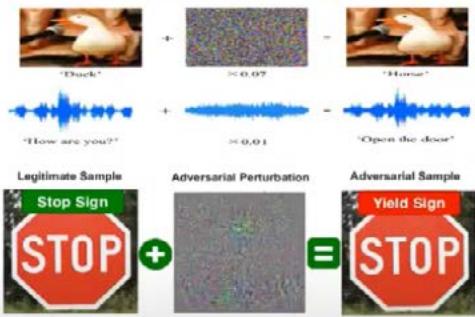


- Often in Security applications one of the classes dominate over the other
- In CCTV footages, abnormal even is very rare compared to non-important events
- Off-the-shelf models fail in these scenarios

- Heterogeneity of samples and class imbalance (rarity of events): a lot of samples from the majority class but few samples from the population of interest (minority) then all the ML that have been built is deemed to fail.
- Missing and noisy data
- Non interpretability of models (Black-box nature of DL)

Adversarial Attacks and Robustness is also an important point of consideration.

Adversarial attacks and robustness



Legitimate Sample + Adversarial Perturbation = Adversarial Sample

- ML models are very fragile in nature
- A small, humanly non-perceivable noise is enough to completely break the model
- Reliability of the models are questionable given these kinds of scenarios

Biases and Non-Explainability:

Learning machine models are highly biased based on the terms of the data that they ceased. For example: it was found that it associates certain criminal activities with one group of ethnicity. it also showed high biases by associating the skill of cooking with women.

Biases and non-explainability



- ML models are as good as the data that they see
- Datasets are created by Humans
- Thus Human biases creep into model biases
- The US judiciary example (biased on a certain ethnicity)
- Models are not explainable – One doesn't know why predictions happen

Possible Remedies:

- Actively collaborating with the end users i.e domain experts and ML practitioners. Learning meaningful representations may provide some respite.
- Methods like Self and Semi supervised learning may help.
- Representations should be learned with expert-knowledge driven priors and regulators.
- Learn cross domain, large scale, multimodal, multi-site representations.

Part - III

»» 15:30 - 15:50 Hrs: Dr. Arun Balaji Buduru, IIIT - Delhi.

»» Topic: Artificial intelligence in Enterprise Security

The fourth technical session part 3 was held from 3:30 pm to 3:50 pm and was based on the theme “Emerging Trends in Cyber Security”.

Dr. Arun Balaji Buduru, IIIT - Delhi, Assistant Professor, Head of Centre of Technology in Policing(MHA)– delivered his talk on the topic “Artificial intelligence in Enterprise Security”.

Dr. Arun Balaji addressed that there are new branches of learning systems which are coming into being called explainable AI. He talked about trust and verified models. Later he mentioned AI for cybersecurity -building generalized learning systems. He gave the example of driving systems for generalized learning. He quoted that if the user environment is dynamic and our requirements are changing, we can adapt with generalized learning systems. He addressed a question of why security is hard. He posed this question to the audience. He concluded that security is hard because of the process of procedure, people and technology. Later he elaborated on how these three areas are influencing security. So, given this paradigm, he reached a conclusion, that no piece of code, no piece of software and no piece of system is 100% secure because every system we develop, deploy, is prone to attack.

- He added that generalized learning systems help to harden the security of systems. He mentioned we all are living in a smart world environment and all of us are continuously being monitored by technology systems which are collecting rich personal data. He spoke about the need to harden our security systems because most of our today's economy is increasingly becoming digitalized and he added that, most of the data getting generated from diverse sources may not automatically translate to actionable intelligence, in fact it makes it difficult. He mentioned integration of different pieces of information to generate actionable intelligence, because some pieces of information are more important than others. He gave examples for recent attacks in security systems using CCTV cameras. He noted that, if the users were weaker in security solutions it would be an issue. Security solutions are only as strong as their weakest links. Later he addressed the importance of AI and ML.
- Networks are growing in complexity, and attack surfaces are increasing- he added the

example of IoT.

- Not enough security professionals
- Humans are slow in responding and decision making
- Massive amounts of data it includes malware, network traffic, process behaviour, user behaviour.

He concluded the speech with a current chart of generalized systems and their efforts and contributions on it.

- Language independent models for emotion detection and speaker verification systems-with attention mechanisms.
- Ongoing validation on real world dataset (for Delhi police)
- Adversarial attacks
- The current focus is on adversarial attacks on computer systems.
- Differential privacy-providing effective trade-off between data privacy and data utility.
- Behaviour modeling of malwares for effective online monitoring of artificial systems.
- Providing security breaches in large networks
- Profiling encrypted traffic.

Part - IV

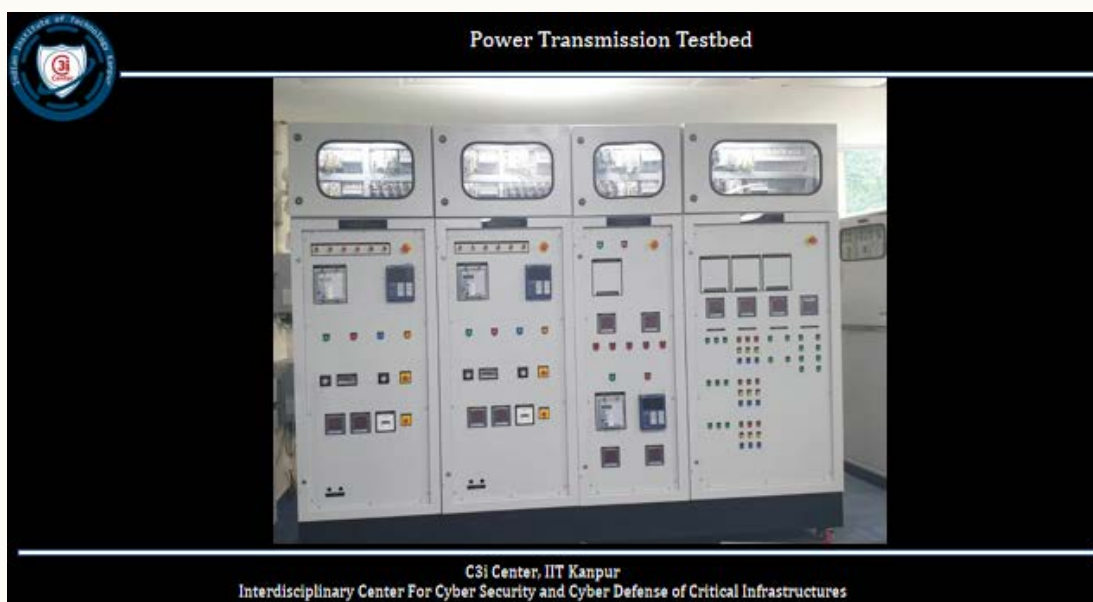
»» 15:50 - 16:00 Hrs: Prof. Sandeep Shukla, IIT Kanpur.

»» Topic: Artificial intelligence in Enterprise Security

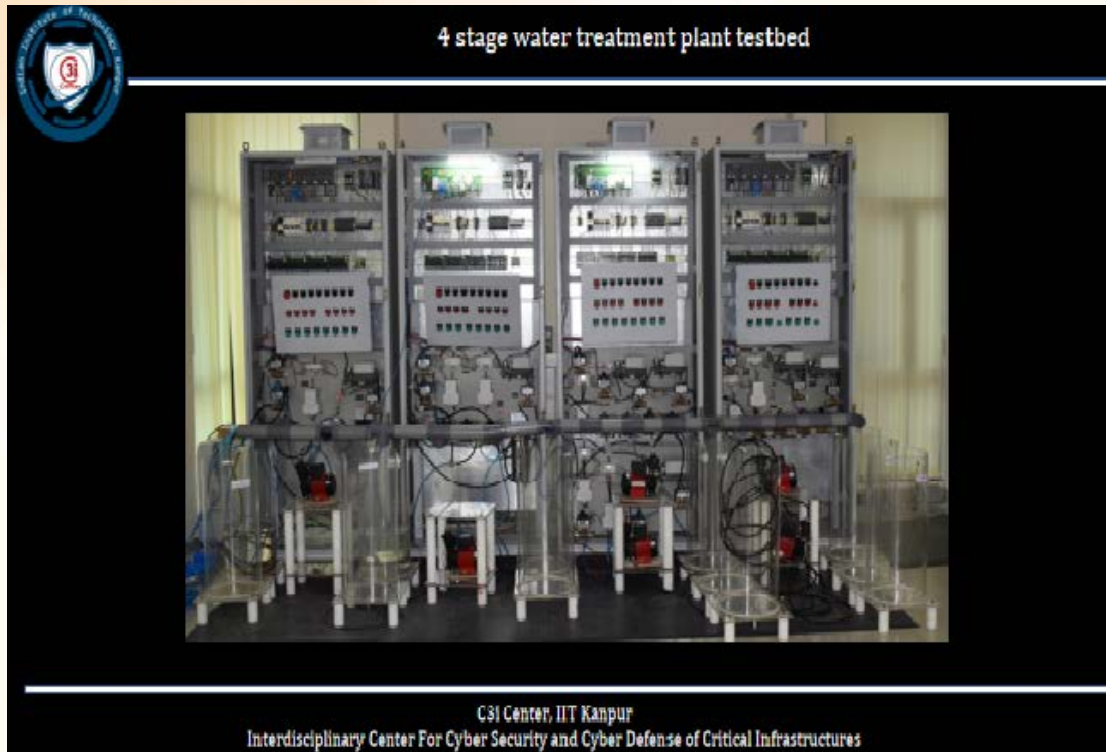
The fourth technical session part 4 was held from 3:50 pm to 4:00 pm and was based on the theme “Emerging Trends in Cyber Security”.

Prof. Sandeep Shukla, IIT Kanpur Department of CSE – delivered his talk on the topic “Artificial intelligence in Enterprise Security”.

Prof. Sandeep Shukla started his talk with machine learning and security research @C3i center at IIT Kanpur. he mentioned that C3i stands for interdisciplinary research center for cyber security and cyber defence of critical infrastructures.



He added that they have 15 vulnerability database entries. for this first need to build a power distribution bed, mainly three phase to single phase. there will be various kinds of critical infrastructure components, and these components connected to data acquisition systems. He gave a clear picture of the infrastructure of C3i Centre.



He talked about power transmission testbed, thermal generation testbed, solar generation testbed, power synchronization between generation tested and campus grid.



Later he added that these systems can be used for machine learning, training, figuring out inclusions and anomalies.

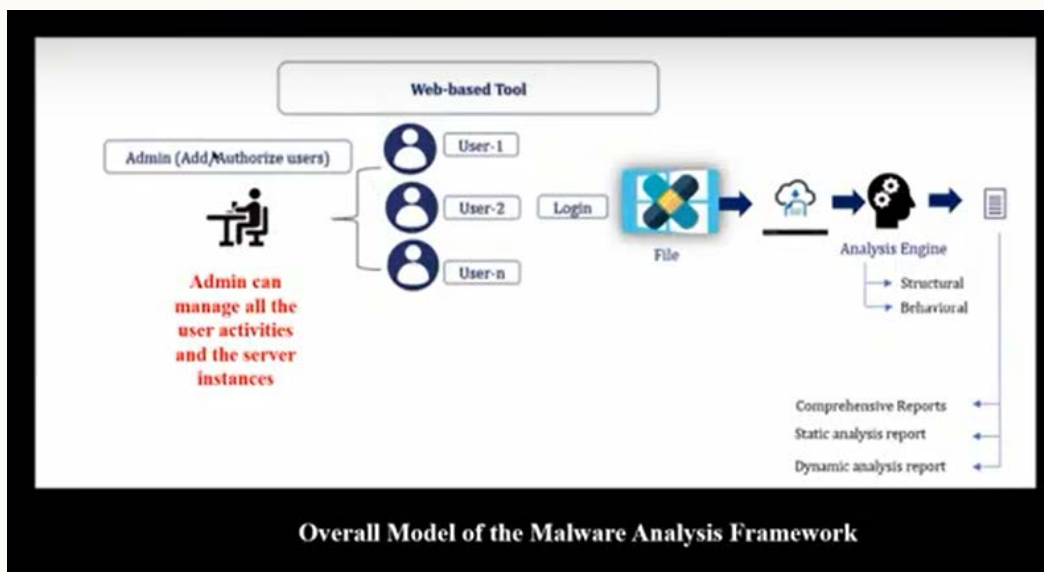
He mentioned a discrete control manufacturing pipeline testbed, that is a 4 stage pipeline and 4 stage water treatment plant testbed.

Then, he spoke about C3i center malware analysis tool pathways. C3i, IIT Kanpur works extensively on malware detection and classification tool development. so far, they have detected the following file types.

- windows executable
- ELF or LINUX executable
- PDF
- APK
- javascript(JS) files
- word document files
- JPEG

He added that as different malware classes exhibit different behaviour, hence this tool learns and predicts the malware based on their behaviour.

Later he mentioned the overall model of the malware analysis framework.



He mentioned the tool's user interface. This is mainly focused on where this malware is coming from, and who is responsible for this malware. He added that organizations are susceptible to facing threats from attackers, be it insider or outsider. Deception is a layer of security which helps the organization to protect itself from imminent threats also, he mentioned statistical and data analytic areas of the SIEM system deployed at C3i center.

Later he addressed data driven IDS. It is a protective mechanism that helps us in capturing ICS behaviour with a large number of parameters and understanding the underlying system dynamic. Also,



he mentioned boiling frog attacks and data cleaning processes.

He spoke about, challenges of destroying IDS for CPS, they are,

- the unavailability of properly labeled data
- not robust to outliers
- weak threat models
- end result must run in resource constrained devices

Also, he addressed the need for robustness. They are measurement errors, inadvertent mistakes, and training data poisoning. Two systems are developed based on denoising autoencoder IDS. This system is unsupervised, discovers latent features, and robust to training data poisoning.

PANEL DISCUSSION

» Topic of Panel Discussion: Industries best practices for top cyber threats to an organisation

Panelists:

1. Sh. Krishna Sastry, Parter, Cyber Security, EY
2. Ms. Rama Vedashree, CEO, DSCI
3. Dr. Nishakant Ojha, Advisor, Cyber & Aerospace Security, BECIL
4. Sh. Vijay Devnath, CISO, CRIS, Indian Railways

Moderator: Sh. Brijesh Singh, IPS, ADG Home Guards, Maharashtra

Sh. Brijesh Singh IPS moderated the panel discussions in CISO/CRO/Intermediaries summit in BPRD headquarters Delhi.

The topic for the panel was “Industries best practices for top cyber threats to an organisation”.

He started the panel saying that technological changes have taken place in the past few years. Nowadays systems are protected by everything right from perimeter defence to endpoint detection and response to people using Artificial intelligence and machine learning for detecting anomalies.

Today working at home and working at home is becoming a reality which is going to stay there for a long time. If we look at what is under threat from financial Cyber crimes everyday thousands of people are victims of cyber criminals right from Phishing and vishing calls involving various banking frauds, malwares etc.

He further said that Shastri has been somebody in the country who has deep experience with actual cases where banking systems have been compromised. And all are not known to the public as India doesn't have a compulsory reporting policy.

He further stated that problems with public order on life everyday something goes viral people are being attacked due to these messages a new look at nation-states critical infrastructure is being attack cyberpower. US was rendered powerless by some ransomware operators there they basically compromised the colonial pipeline and declared a state of emergency.

ISO 270001 certificate auditing and other hardening measures are being followed by organizations yet why attacks are still happening are there any measures required by organizations to adapt? He questioned the panel members and requested Shastri to give his views on this topic.

Krishna Sastri had said that in the last 15 months more than 40-50 cases which really targeted the bank systems were investigated under him. He further talked about advanced persistent threat attacks which are a highly focused attack where the threat actor was present for 9 months. The organizations were not in a position to detect.

The best practices were really missing. He further emphasized that around 8 to 9 years back attackers used to exploit some internet-facing server, any vulnerability to that from the web server to the application server. It took days to go for a database server because they then followed something called 3 tier architecture.

He continued saying that in 97% of the cases the source of infection is nothing but the endpoint



machine where an employee works on the system. Taking example of Cosmos Bank breach their branch Computer System was attacked and from there the attacker reached the system the attacker was able to penetrate the whole bank network.

Today the major source of infection is nothing but phishing mail which they send to an employee who doesn't have proper cyber awareness.

The endpoint security management is important and should not be neglected as the attacker can via lateral movement move around the network and thus achieve their goal of data exfiltration.

Lack of forensic readiness is one major concern in organizations observed Shastri the organizations did not have the knowledge about the logs that should be captured, what format should the logs be in and what is input to a SIEM.

Without proper logs SOC security operations center would not be alerted.

Identity access management is important and having logs and log collectors is of utmost importance.

Sh. Brijesh asked about misinformation and disinformation and how it will be used as information warfare.

Dr Nishikant Ojha discussed information warfare and how important it is to understand that everything is secured and nothing is secured. He talked about developing cyber security sensitivity among policy makers and the IT practitioners of organisations.

Sh. Vijay Devnath emphasised on the need of data backup. Encryption should be provided to confidential data. He continued speaking about the importance of having human backup also. He cited a hypothetical instance that despite having all backup plans and infrastructure but the human resource responsible for managing everything is on leave. So in such situations nothing would work. Another important aspect of back-up plans is that it should be distributed in various regions and zones so that if any attack happens that damage can be minimized. While commenting on the existing education system, Mr. Devnath said that our curriculum should include cyber and cyber security education. He also pointed about the importance of including cyber safety penalty rules within the organisations so that cyber negligence by employees which result in massive mayhem could be penalised.

Smt Rama Vedashree spoke about the cyber risks being accentuated in the post covid world. She said that even banks that are well matured in implementing robust user enterprises woke up to the evolving cyber security risks during the lockdown periods. Securing end point systems are the biggest challenge for corporate companies. Even engineers of IT companies became victims of phishing attacks. The business continuity plans were never tested for the situations created during covid pandemic. This led every CISO and CRO to revisit their BCPs and re-strategise business resilience. Business resilience risks need to be looked at far wider risks than mere technical risks. The priority of large enterprises in current times is about securing the end point devices which are beyond the traditional firewall of their network. Significant workload has moved to cloud networks. Industry leaders in India have now realised the fact that cyber risk is the biggest show stopper to their business continuity and business growth. CISOs have now become business leaders. Smt Vedashree also mentioned that companies are also doing cyber security mock drills where phishing emails are sent to their employees to test and train their cyber awareness aptitude. On the capability side also the Indian IT companies and product companies are showing their maturity. Many cyber security product companies are serving Indian and global customers.

DEBRIEFING SESSION

Sh. Bhola Shanker Jaiswal, IPS, IG/Director (Training) presented his debriefing session.

The first technical session held discussion on the theme “Critical sector related Risks and roles and responsibilities of CISO/CRO”. A detailed deliberation took place on the topics of ‘Emerging cyber threats and mitigation measures for CISOs’ and ‘Cyber security in modern critical information infrastructure’. Experts mentioned the importance of having robust and strategic business continuity plans, having the know- how of end to end network infrastructure of an organisation and the best practices of protecting the legacy infrastructure from modern day vulnerabilities.

The second technical session was organised to deliberate on the theme of ‘Best Practices in Cyber Security’ and three different sub-topics were discussed viz. ‘Secure Cloud Services’, ‘Secure Network Infrastructure’, and ‘Challenges in Prevention and Mitigation of cyber threat’.

There were three different technical sessions post lunch in the conference.

The third technical session was based on the theme ‘Securing Critical Cyber - Physical Infrastructure’. This session had detailed presentations, talk and discussion by the eminent experts from LEAs and industry on the topics of ‘Secure Online Public/Financial services and Citizens’ Data’ and ‘New Perspective in Cyber security for LEAs’. The experts talked about the importance of robust data protection strategy, cooperation among various stakeholders in combating cyber crimes and tackling cyber security challenges.

The fourth session included the discussion on the theme ‘Emerging Trends in Cyber Security’ and delved into the research and development being undertaken by leading academia on the subjects of ‘Zero Trust Model for Security’ and ‘Artificial Intelligence in Enterprise Security’. Leading academicians of the country explained to the delegates about the role AI and ML are playing in human lives and how they are posing the ever evolving challenges of cyber security for LEAs. They explained that ML is not foolproof and the Explainable AI is the way forward. The discussion also revolved around the R&D based solutions academia is developing for LEAs in cyber crime investigation, cyber crime prevention and digital forensics.

The final session was a panel discussion on the topic ‘Industry's best practices for Top threats to an organization’. The panel discussed endpoint protection, active directory hardening, machine is something which can protect us to a certain level only. Human aspect is needed in cyber security plans. Business continuity plans should be robust and tested. Phishing emails are used as the first line of attack. Business resilience strategy. Mock drills of cyber security are the need of the hour.

The conference ended with a vote of thanks by Dr. Karuna Sagar, IG/Director (Modernization).

GLIMPSES OF THE CONFERENCE



















National Conference of CISOs/CROs and Intermediaries





















CONTACT LIST OF BPR&D OFFICERS

Name of the Officer	Ph. No.
Sh. Karuna Sagar IG / Director (Mod)	011- 26782023
Lt. Col. Ashwani Kumar AD (Mod)	011- 26782183
Dr. Ajit Mukherjee, PSO (LS)	011- 26734938
Dr. Raveesh Kumar, PSO (W)	011- 26785451
Sh. Sushil Kumar PSO (B&E)	011-26734931
Dr. M.M. Gosal, SSO (T)	011- 26734815



officialBPRDIndia



BPRDIndia



Bureau of Police Research & Development India



bprdIndia



www.bprd.nic.in



Cyberdost



www.cybercrime.gov.in



NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC) BUREAU OF POLICE RESEARCH AND DEVELOPMENT

Ministry of Home Affairs, Government of India
NH-8, Mahipalpur, New Delhi-110037