"ACCELERATING BUSINESS TRANSFORMATION MEANS ACCELERATING CHANGE MANAGEMENT STRATEGY"

These days we are observing that businesses are undergoing a transformation at a rapid pace. The definition of accelerating business transformation varies among organizations. Dr. Sanjay Bahl, CISM, CIPP/IT, CERT-In has vividly elaborated the meaning of accelerating business transformation. Dr. Bahl is also an adjunct faculty with IIIT Delhi. He has been providing consultancy in the area of governance, risk, compliance, security, privacy, forensics, investigation and fraud management to some national level projects in India. Prior to CERT-In, he was the Chief Security Officer (CSO) for Microsoft Corporation (India). Prior to joining Microsoft, he has also worked with Tata Consultancy Services (TCS) as the Global CSO.

In his words, "Accelerating business transformation means accelerating change management strategy, which you can define as accelerating any shift or realignment or fundamental change in business operations. Why is this acceleration required now, so that the business can survive and thrive in an environment which is throwing up new innovation driven opportunities as it responds to shifting market demands, while navigating the evolving regulatory complexities. This survival of the business is now dependent on maintaining trust in these services that it provides."

DR. SANJAY BAHL
Director General, CERT-In

THE AAJA ENVIRONMENT

At present we are living in a volatile environment which Dr. Bahl mentioned as AAJA. Further elaborating on this he said, "We are living in an AAJA environment. It is Asthirta or volatile. It is Anishchita or uncertain - lack of clarity about the present and the future. It is Jatilta or complexity - the multiple factors which are impacting key decisions. It is Ashspashtta or ambiguity - lack of clarity about the meaning of events. So, why is it now that we require this acceleration of business transformation because now we are living in this AAJA world and this is an extraordinarily challenging time, where this pandemic has given rise to a contact free economy which is accelerating digital business transformation and it is changing our society, government and industry. So, businesses are now taking informed data driven decisions and making choices which have the potential to shape our economy, politics, Digital India, culture and society. We need to decide what kind of society, government and industry we wish to create rather than trying to foresee the kind of society, government or industry that will be created. So what would be the building blocks for digital transformation? It requires connectivity without it obviously there is no digital transformation. Once you have connectivity, the tools etc. then you should know how to effectively use them. For that you require skills. Once you have these, you need some policies to address the security and privacy issues in the digital transformation and also you need governance and strategy coordination."

UNDERSTANDING THE THREAT LANDSCAPE

Understanding the threat landscape is very important without which it is difficult for organizations to provide necessary security capabilities. Discussing it Dr. Bahl said, "As a business leader, you need to understand the threats which your organization will be facing including your people when they are working from home during these times. You have to provide clear guidance and encourage communication from them, so that they ensure that the policies are clear and easy to use when they are working from home and they know whom to contact if there is any issue or suspicious activities they notice. You have to provide the right security capabilities in the sense that whatever machines or digital devices that you have given to the employees, they are managed from a corporate perspective and you have the necessary tools on these digital devices, so that the people are not impacted when there is something malicious happening.

As I said that, you have to understand the threats and what is the threat landscape at present? What we see is that there are nation state actors who are involved in espionage operations and also financially motivated crime and frauds. There is targeted ransomware which is available as a service, destructive malware, remote login, credential stealing memory executable ports - attacks which are increasing, also on the increase is the distributed denial of service attacks frequency. With the entry of IoT or Internet of Things, the attacks have also increased. Also, there is an observation on traffic, the internet traffic being hijacked. On the crime side, the ecosystem is demonstrating extreme flexibility in terms of the tactics, techniques, procedures they use and are able to change their course mid campaign to achieve their objectives."

SECURITY GOVERNANCE

Talking about security governance he highlighted, "There is obviously a challenge in terms of trust in the digital devices and connectivity. To address it in a holistic manner, you need to look at the governance. When you look at governance, I am specifically talking about security governance because security is a quality aspect. So security governance has a direct impact on the security service quality and also on the organization's performance. The services that you have to provide should be resilient, you are seeing what happens if the services are down or for a few days, if you are not able to get connected and not able to do your business activities, you have to face huge losses. Your policies should be in place for security and privacy. Whatever software you are developing will have to follow a secure software development lifecycle. You also have to look at the operational aspects in terms of the security and safety operations center that you have depending on the size of the organization. You should be able to integrate all your different devices from a security perspective, including all the supply chains so that you have complete visibility as to what is happening and what is the threat that is emerging and from where. Once you get all these then you will be able to provide value added services which will improve organizational performance and also provide a better user experience."

ZERO TRUST ARCHITECTURE& CYBER-PANDEMIC

The Zero Trust Architecture is a new approach to security, discussing on this he said, "There is a trust deficit in technology based systems which has increased during the COVID time. So there is a new approach known as a zero trust architecture. This architecture is a security concept fixed on the principle that organizations need to proactively control all interactions between people, data and information systems to reduce security risks to acceptable levels by creating discrete granular access rules for specific applications and services within a network.

Basically, cyber-attacks erode customer trust. The cost of the cyber-attacks has increased 52% and the primary goal of it is service disruption and infrastructure destruction. It is mentioned in various reports that Ransomware attacks will occur in every 14 seconds and create a loss of $11 and a half billion. These cyber-attacks are becoming more frequent and impactful because they are impacting the digital infrastructure and that is why they need to be robust and resilient, otherwise this foundation itself will be shaken. It is impacting digital confidence because confidence is comprised of transparency, trust and security. Finally, it is impacting the digital economy because with fractured technology or infrastructure, the economic growth will not be sustainable. So what will happen if there is a cyber-pandemic? If it has a similar characteristics of the Coronavirus, then during the cyber pandemic it will spread faster and much further than any biological virus. This has been mentioned by the World Economic Forum. The reproductive rate of COVID-19 is somewhere between two to three when there is no social distancing and this number reflects how fast the virus can spread. If we contrast this with a cyber-pandemic then it is estimated that the reproductive rate of the cyber-attack is 27 and above. You have seen what damage two or three has created by this biological virus and what will happen when there is a cyber-pandemic which impacts 27 and above. The economic impact of this widespread digital shutdown will be of the same magnitude or maybe greater. In a single day, without the internet the cost to the world will be $50 billion. So if you have a 21 day cyber lockdown that will cost over $1 trillion. The recovery from this widespread destruction of digital systems will be extremely challenging. So, just imagine replacing five percent of the world's connected devices which may have been impacted by a malicious software etc., will require about 71 million new devices. And how do you get these new devices? Suppose the manufacturing and logistics systems are also impacted, is there a mechanism to manufacture and produce so many new devices on an urgent basis and then whatever has survived can you at breakneck speed patch and reinstall whatever has been impacted? These are nightmares that we are sitting on."

BUILDING TRUSTED BUSINESS INFRASTRUCTURE

Building a trusted business infrastructure is important and Dr Bahl explained how to build it, he said, "So how do you finally look at building a trusted business infrastructure? I will say there are six basic things - five pillars and a foundation. One is having a trusted supply chain. You need to make sure that you implemented a trusted value chain framework where you are in a position to do security testing of the framework, equipment and software which is coming in through certification labs, to carry out risk analysis to understand how much is the risk, whether you are willing to accept that risk, are you willing to outsource that risk or mitigate it. That will define who will be the trusted supply chain partners and how you are going to interact with them. You have to look at a trusted architecture where you identify and adopt standards. The zero trust architecture which you will have to probably look at, also the managed service providers as part of your trusted supply chain and a trusted architecture because now they are going to be sitting inside the business architecture. So, how secure are their infrastructure, processes and the people, you have to start addressing those issues.

Next will be robust and resilient infrastructure in terms of network monitoring, detection of attacks and outbreaks etc., information exchange or any attacks and security issues or anomalies because no one is in a position to do everything on their own, you will have to start looking at partners."

CERT-IN INITIATIVES

Dr. Bahl talked about various initiatives of CERT-In. He said, "From the Indian Computer Emergency Response Team or CERT-In we have put in place various projects which are helping a variety of organizations and sectors such as the Cyber Swachhta Kendra, which is providing service on a daily basis like which are the devices that have malware, which are the vulnerable services that are to be looked at by your organization.

We have the National Cyber Coordination Center which is in a position to look at situational awareness and give advanced notices as what is happening, what you may want to do and what steps you may want to take. We are providing Cyber Threat Intelligence using the S TIX and TAXII format so that there is no manual intervention. As soon as we understand what is the threat, we are providing the indicators of compromised, the details that can be ingested by our SIEM's etc. directly, so that there is no manual intervention and there is no scope of error and the devices are then appropriately secured and this is almost in real time.

Security by design is the next pillar, where you are looking at compliance and adequacy of security controls. We have empaneled auditors in place - more than 90 of them today. We have put in place the Cyber Crisis Management Plan. So when there is a crisis, what needs to be done, who needs to be informed and how you need to carry out what activities, there is an incident response so that you let us know that this is the sort of incident that has happened and we will provide you guidance. This is a 24/7 operation. You will have to participate in various drills that we perform and or exercises which helps you understand what your security posture is, where you need improvements, how good your people are, how good your processes are, how good your tools are.

The fifth pillar is capacity building because there is a huge gap in terms of what skill set available with people and what is the skill set that is required. One way is obviously the skill set which is required for securing all this infrastructure and devices. So, that is the technical skill, but you also have to make sure that you build capacity across the organization by letting them know what they have to do in terms of security and how they need to make sure that they are not falling victims to simple things like phishing etc.

So, there are mechanisms of carrying out these awareness sessions. One is you can do it yourself, there are various other entities doing awareness sessions, then also for the technical people, there are formal courses, which are available and certifications and the foundation for all this is the ecosystem which needs to be in place where we need to look at the academia which can come up with certain research and development aspects which can help and feed into this whole system. We need to look at the privacy impacts, we need to create more auditors."

GRIEVANCE AND REDRESSAL SYSTEM

Talking about the necessity of grievance and redressal system, he concluded saying, "Obviously, when you are providing services, there might be grievances. So, you need to have a grievance and redressal system because now you have gone digital. So, you have to start addressing the grievance redressal systems for privacy. You should have someone to contact in case there is a privacy impact for the users.

Since you are looking at multiple partners in the supply chain, you may have to carry out background checks not only within your organization but also across the supply chain and ensure that there is no issue and challenges from that perspective. Also look at how you can, as the honourable Prime Minister has been saying, look at products and services which will make our go towards Aatmanirbhar Bharat, Make in India which will help you in doing some of these things.

So, I think if you have these things in place and look at security, you will have a much better organizational performance. A proper security governance and the results will be obviously available to all and you will be able to look at the requirements of innovation which have come up during these times. So these new opportunities which have been opened up and you will be able to address the market demands and be compliant to the needs of regulations which are evolving and coming up in place."

COVID-19 BROUGHT THE BIGGEST TRANSFORMATION THAT MANKIND HAS EVER SEEN

As remote working has become the new normal with the outbreak of Covid-19, cybercrime has reached to a new height. In a chat with VARINDIA, Cyber Security Guru, **SANJAY SAHAY, IPS - TECHNOLOGY EVANGELIST** has shared his views on the current scenario of cyber security, while remote working is the new normal. Though chosen voluntary retirement this year, Sanjay is serving the nation with his expert commentary on cyber security trends and cyber policies. Post graduated from St. Stephen's College, Sanjay through the course of time became a technology evangelist.

According to him, "Today we are living in an age of digital transformation, but unfortunately as seen in the last 20 years, the industries were never able to accomplish this transformation before COVID-19 break through. The pandemic forced us into this digital transformation. Everything has converted - our world, fun, entertainment, communication, watching movies, banking transaction, our intimate social interactions into one single gadget. This is a new paradigm, home and laptop have become the harsh realities of today's existence.

To live in a safe and peaceful manner, responsible digital learning is required. While people will be able to exploit the benefits of the internet age, they also learn how to navigate the digital world without getting exploited. Cyber Security today is as complex and as an enterprise. The business world exists today on cyber security."

VULNERABILITIES OF 'IT' ECOSYSTEM

Nearly 74% transition is not happening to the most secured gateway because of the security purposes. Today, all over the globe IT behemoth is happening on the cloud. IT ecosystem is a very complex network where at large points vulnerabilities arise. Sanjay says, "To take care of this old vulnerability end to end can be precisely called a cyber-security. It might be caused due to data, servers, port, and lack of patch management, organizational culture or the lack of direct training imparted to that particular individual. It might be because of any other physical factor too. There are instances wherein physical factors have played a key role."

From Sanjay's point of view, at first an organization's CIO, COO or CEO should know the nature of cyber security it requires. If they do not understand the requirement of their organization then there is a chance of cyber breach. "Until and unless we understand the old data lifecycle from the company's creation, last usage interface, it will be extremely difficult to understand what will be the nature of cyber security. There are standard systems which are operating all over the globe. It is also happening that cyber security is getting weaker by the day." Sanjay says.

He further added, "We are living in an age where cyber security is a very dynamic field. It changes with the nature of connectivity, nature of human resources to employ, train, recruit and develop. If you are not ready to understand and learn, all the standards will become next to impossible to keep yourself set. A decimation of most of the enterprises happens because of the lack of cyber security. MS Office is the largest targeted software, nearly 70% of the attacks happen on it. Nonetheless, all of us use this because we do not have a choice."

ALWAYS BE READY FOR AN ATTACK

Warning against the cyber-attacks, Sanjay says, "Everyone connected to an enterprise is not able to understand the cyber security ecosystem. The persons who are providing the resources are also unaware as to what they are providing. This is the crux of the problem, the subset where security experts stuck up and go for a management approval. They are not able to explain that in case of a cyber-breach. The earliest or the average time needed for that particular detection is around 200 days. We have to be always be ready for an attack. And the more you prepare in better place you are. So that is the strategy to an undeclared war, which is going on. Hackers have to look for only one gaping hole by which they can attack and we have been hearing of these attacks over and over again."

RESILIENCE IS THE KEY

As attack is obvious, Sanjay suggests having resilience. The CIA Triad (confidentiality, integrity, and availability) is the key on which the whole functioning of the enterprise runs. He says, "It is your capability to bounce back into business in the shortest possible time, at least with the skeletal services, this is the capability which all the customers are looking for. Nobody will believe that they are absolutely safe and nothing is going to happen. Even if it does happen, you have the capability to safeguard at least the most vital of all information. Cyber Security has to be factored in the company valuation. You have to understand what are the goals, the processes and the impact. As all of these are combined, you will get a situational awareness with COO and CEO. If you get into a medium sized company or a big company, you realize that basically only 28 to 200 software solutions on cybersecurity are functioning. The software solutions are running in different parameters for different sectors or servers or network for software applications. Literally, nothing can give you the whole cyber security stance of your enterprise on one single network."

RANSOMWARE & DATA BREACHES

Sanjay finds out that the length between ransomware and data breaches is continuing to blur every single day. At the back end of the ransomware attack, it is a phishing attack. "It is spearfishing people who deserves position, power and capability to give you all that data access by fooling. Ransomware having the capability to get into your data and literally encrypt it in a manner which will be next to impossible for you to do anything with that. In this Covid-19 situation, nearly 11 big data breaches have occurred costing nearly $144.2 billion. COVID-19 has changed completely everything. It has been the biggest transformation mankind has ever seen. Also, the biggest digital transformation, which we have always visualize and the company has always wanted to happen." comments, Sanjay.

PANDEMIC & HACKING

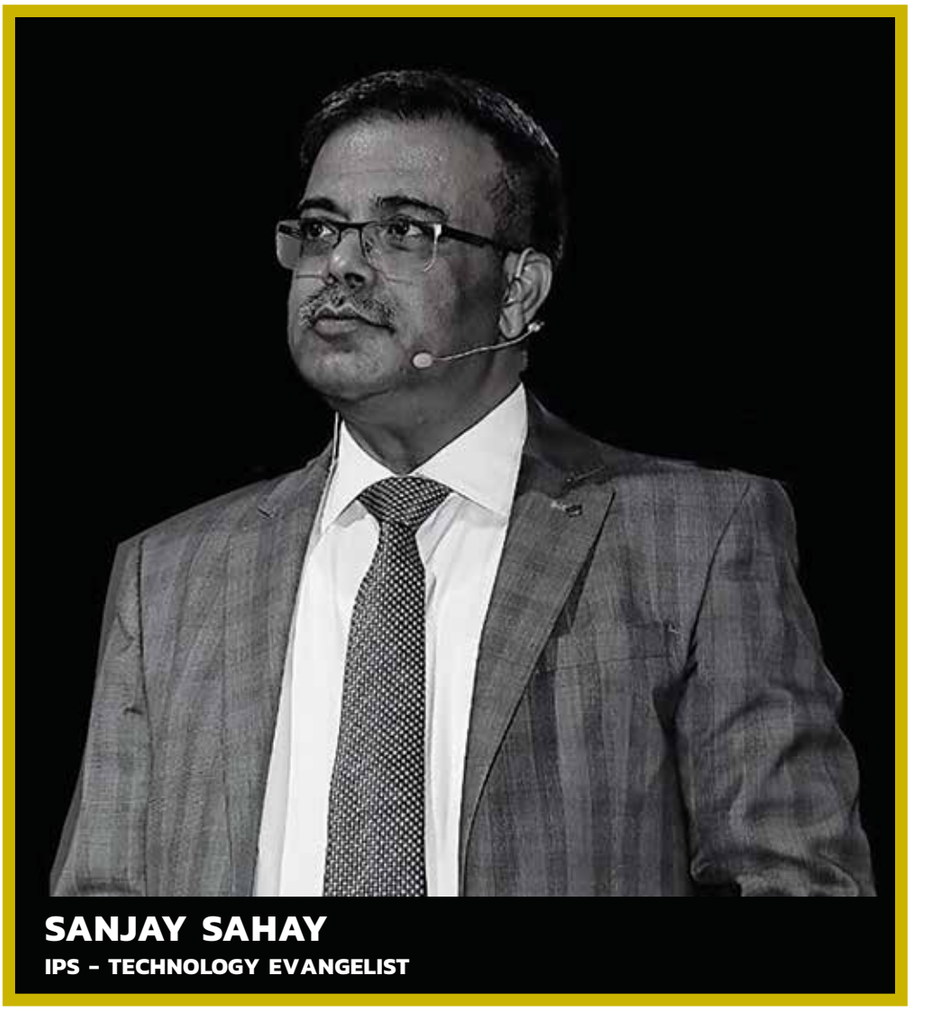
Talking about the current hacking process, Sanjay says, "As we talk about data breaches, this particular year 80% of the breaches is due to COVID-19 websites. The COVID-19 websites may relate to helping COVID-19 patients to

> "A very integrated support system is needed now, due to the work scenario, not only data center is needed but Disaster Recovery Center is also needed. Work from home brings in a totally different environment; the office environment was secured from the digital point than the extension to home."

support, help and lots of other areas. Most of them have some element of cybersecurity compromise. Once you click on that particular payment or any way it goes through the wrong direction and reaches to the hackers and most of these downloads or links are connected to something which is nefarious. As all of us are scared in this current scenario, we tend to get into that particular maze and once you click onto that attachment, then the situation is totally different. I have received a lot of complaints from people who have been frauded and cheated in this manner. Health sector is primarily under severe attack."

A very integrated support system is needed due to the work scenario, not only data center is needed but Disaster Recovery Center is also needed. Work from home brings in a totally different environment; the office environment was secured from the digital point than the extension to home. People started to roll over to the private network everywhere, using their gadgets. But big companies have provided infrastructure to their employees. Though they are safe in that infrastructure but remote working has given rise to cybercrimes.

Sanjay, perceives, "We are basically sitting on a virtual digital landmine or worker landmines. There are lots of things where the stuffs do not get the right sort of the connectivity because of the public WiFi. Most public Wi-Fis can be compromised earliest in the process, the employee and the company both can be hacked."



SANJAY SAHAY
IPS – TECHNOLOGY EVANGELIST

RISK ASSESSMENT, THE RIGHT WAY

Stressing on the risk assessment first, Sanjay says, "You have to treat all these factors as a part of your risk. Risk assessment in the post pandemic time, or in the penalty phase should be documented. If you do not know the risk itself, there is absolutely no strategy by which you can mitigate the risk. We have lots of work force which is being referenced; these people who are moving out of companies, they are certainly carrying a grudge. They are nursing a grudge that injustice has been done to them. If they fall into the wrong hands, they might leak secrets, or might become cyber criminals themselves. So we have a whole load of floating, unemployed, cyber enabled people who are there in this world. The Business Continuity what has to happen in the pandemic is very different to what you had imagined as a part of the business. There was hardly any business continuity plan, where pandemic was a part. We are left with no choice but to create a business continuity plan with pandemic incorporated. So the whole digital scenario from the utilities, tools, hacking groups, the ledgers to equity , to ransomware, quality of the encryption use, the capability of these people and the capability of lack of attribution, all of these things have messed up the whole scenario. Another year not left with much choice, but to work in a much dispersed digital environment in which we never find our way."

AT LAST

The way to handle cyber security is important; it has greatly increased the functioning of the security experts. Their very existence is based on cyber capability and robustness of cyber security. Enterprises help that business capability to deliver everything actually hinges on the capability of cyber security. Any hack brings those capabilities down the trust and loyalty to that particular brand. Giving an example of a city of Belgium, Sanjay describes the process of ransomware and how it is affecting not only common people but also the government. "It was a mega ransomware attack, and the whole government out of their senses on that particular point in time. The attack affected nearly 1 billion computers in the U.S. in a while. The attack is an outcome of lack of management for monitoring. In the history of cyber security it has been seen that ransomware attacks happened only in cases of a large number of public utilities is woven in the company. The money had to be paid due to the cyber incident. But there is no way to solve the problem. Government agencies, municipalities or private companies which are mostly public limited companies hit by this kind of attack. I do not think to pay them is the right kind of approach. Resilience is something which we are not working upon. After two years, when I presume that the whole patch management will happen not only in India but also in a place like U.S."

In this way, Sanjay has correctly estimated cyber security, where the security leaders are placed, what is their capability, how they move forward.

> "We are living in an age where cyber security is a very dynamic field. It changes with the nature of connectivity, nature of human resources to employ, train, recruit and develop. If you're not ready to understand and learn, all the standards will become next to impossible to keep yourself set. "

A WALK INTO THE CLOUDS OF "IT" EVOLUTION: A WAY BEYOND BIG DATA & CLOUD

Cloud architecture has evolved to emerge the most topical IT paradigm in the recent times. Cloud is rapidly transforming the IT landscape. The cloud has several unique architectures and many more are still evolving. The primary ones are the SaaS, PaaS and the IaaS that can be deployed on private, public, community and hybrid clouds. In a chat with VAR India, Vipin Tyagi shared his views on Cloud Architecture.

Vipin Tyagi, a name associated with innovation is also an industry veteran from Information Technology and Telecommunication Industry, Executive Director at C-DOT, Tyagi has over rich three decades of versatile hands-on experience in R&D, convergent networks; and development of HR and quality systems. He has a deep understanding of Telecom/ Datacom and Convergent Networking and wireless technologies. In other words, Tyagi can be described as Entrepreneur with new business ideas.

While speaking on IT Evolution Vipin said, "As we all know that traditional business model were rigid, siloed management, labour intensive, the computer and storage were in focus and then we moved to Cloud because of virtualization where the service is anytime and anywhere, no problems with the network etc. and then load sharing and sharing of resources were possible, large scale hardware and software can be put wherever you want, consequently Big Data came in. We still have siloed management but what happened is that we had difficulty in admission control which causes security issues. Consequently, we came to a situation where we had a multi-cloud architecture and then now what I am proposing is that we should go for cognitive self-aware application. Multi-cloud management is an integral part of the basic functions of building block – the security, privacy and transparency. We are doing it because of cost, availability, scalability, manageability, energy consumption and load fluctuation, complexity of managing the whole thing, latency and quality of service."

VIPIN TYAGI
Executive Director, C-DOT

5G- its pros & cons

Even though everyone is speaking about 5G, that is coming up next, but then, no one really speaks about the situation IT architecture will face on 5G arrival.

"5G is Denser with 10 M bits per sec/m3 and 10 M devices/square KM. It is quicker in response, as quick as 1ms including delay of transmission. Also the data consumption is bigger as much as 20 Gbits and user experience could be around 100 Mbits, moving at the speed of 500 kms /minute. More diversity- As slicing of networks for more different applications and Greener as 100 times less power consumptions," are the five Goals set out, according to Vipin.

Speaking further on the goals met on Cloud Architecture he says, "5G is dense, as it comes from various aggregated devices; it is not possible to handle 5G. IT might be able to handle bigger data consumption as applications like YouTube are running, so it is possible that it may handle bigger data consumption, by upgradation. The work on proper architecture is on at the moment.

More diversity is a possibility. Also, with the current kind of web practices, 100 times less power consumptions (Greener) is not possible too".

According to Vipin, today's Cloud Architecture is based on Distributed Databases.

He believes, "Three things are very important: Constituency, Availability and Partition Tolerance, in other words it is called CAP. The theorem is also known as Brewer's Theorem. A distributed database can guarantee only two out of three characteristics.

Most of the CIOs believe that it is difficult to overcome the microservices environment. Data storage is becoming tough for them and so finding database has become difficult. For modern applications, one needs to choose a database that can overcome the challenges of microservices in order to fully unleash the benefit of today's agile development technologies.

"Strategies need to be adopted. Engineers need to overcome the theoretical limit by engineering solutions," said Vipin.

Moving further on Cloud Architecture, he pointed out a few points that what constitutes today's Cloud Architecture.

Evolution of Cloud computing to multi-cloud

The layers of rigid infrastructure, conventional computing, Cloud computing and multi-cloud are available.

"Complexity cliff is scaling the number of compute elements which needs more servers, which is not resulting into same efficiency.

The evolution has actually created complexity:

Practise of adding more hardware actually reduce efficiency.

Returns start diminishing due to overheads and complexity. Response to real time events like sudden increase in demands create problems, spike in demand is not matched by reconfiguration speed to automated fashion."

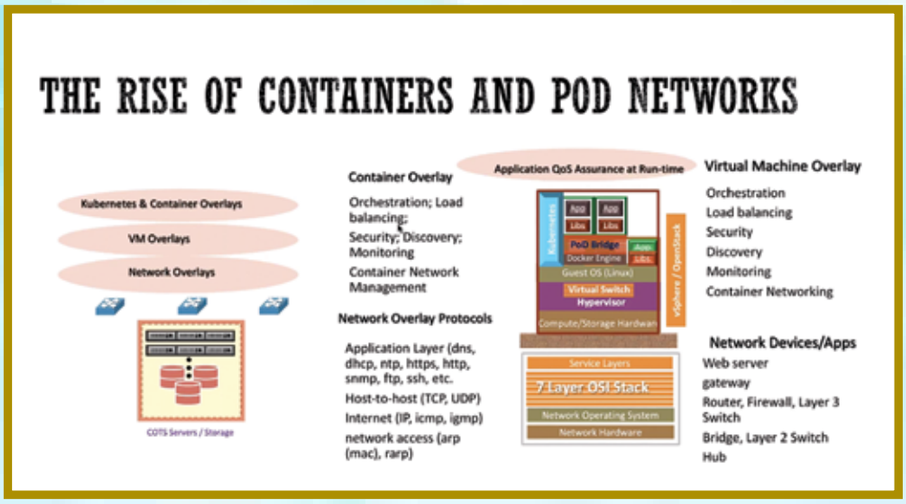
The Rise of Containers & POD Architecture

Talking about POD architecture Vipin said, "There are different kinds of devices that come along. One manages micro services through Kubernetes and Container overlays.

Within POD architecture one has distributed database layer which is more consistent."

Explaining the concept he said, "Computing is a form of ubiquitous computing that perceives the environment using sensors.

A common use is to construct word model which allows location aware or context aware applications that have their own ways of understanding and that are how the context is created. The key considerations are how to demand and define fluctuations.



Another important consideration is admission control strategy to optimise efficiency performance and availability during spike of demand.

Everything has its limitations. One cannot allow everyone to come all the time, but must have admission control. Explaining further he said, It does not mean block all people all the time, but it must have some degree of admission control. Everyone at the same time wants to access one particular place, and then there is going to be an issue. The application should be able to say by itself".

Four Es of Cognition

Elaborating on the four Es he said, "Embodied (cognition is inside the body), Embedded (it is very much inside the body, Extended, for example as everyone do not remember the all contact numbers in the phone, hence phone too becomes a part of one's extended cognition. At last, Enacted cognition: One learns when one interacts. Action is the fundamental for learning".

On Evolution path towards life after Google

"If applied, we had to move on from concurrent synchronous distributed workloads to asynchronous distributed workloads. That means workload has to be in a synchronizing nature.

Next is Global constituency and local autonomy with hierarchical intelligence and four Es cognition. It means whatever one does has to be globally consistent, that means one cannot have different way of handling different notes and entities.

In order to model intelligence in the digital world, the first thing is to go beyond limitations of symbolic computing by infusing cognition and sentient behaviour to address fluctuations, and the availability of resources without disrupting the computations at hand. No shared storage required across multiple clouds".

The theory of oracles and structural machines offer a way to implement hierarchical cognitive overlay that allows to distributed computations to manage themselves and their interactions with other systems, the environment with global knowledge and local control. Behaviour in one component can be changed through message communication.

Structural machines provide a framework to address computational functions (algorithm or tasks that can be described), structure and fluctuations by infusing cognition through cognizing agents to create sentient behaviour.

A new Information Processing Architecture is required for the machines that are created for modelling that are for cognitive systems. Next cognizing agents are put into structural machines. Then the outcome is deep learning or deep knowledge", he believes.

Finally, Vipin concluded his speech on -

New IT Architecture Consideration

"Cognition, Sentient Computing, POD architecture- POD is well known as it is commercially available as of now. Brain Modelling is the influencer.

He also spoke on Markov Blanket i.e. Separation of local states with external state of model. It defines the boundaries of a system (e.g. a cell or a multi-cellular organism) in a statistical sense.

"Deep learning to sustain during fault configuration, accounting protection, security and hierarchy of functions and communications modelling" he said on his concluding speech.