VARINDIA CYBER & DATA SECURITY SUMMIT 2021

CDS 2021:

BE ACQUAINTED WITH TODAY'S CYBER SECURITY THREATS AND ITS IMPACT

Technology has become an increasingly integral aspect of the workplace and society. From email correspondence and financial transactions, to professional networking and collaborative work documents, businesses rely on technology to be connected at all times and conduct work effectively. However, when these lines of communication are threatened or even compromised, it can have a disastrous effect on the business. All businesses, no matter its size, need to ensure everyone involved in the company is up to date on the latest cyber security threats and the best methods for protecting data.

The 5th edition of Cyber and Data Security Summit 2021 (CDS) witnesses an overwhelming response from the industry leaders. Most of the corporate who are into security say that, security is foundational to everything we do as the Cybercrime damages will cost the world $6 trillion by 2021. The pandemic was a difficult test for the technology leaders and the success based on how they navigated their organisations through changing consumption patterns. In this CDS 2021, we have understood from the crème de la crème from the Industry, Corporate world and the policy makers what will be the trend in the coming year and how the leaders are prioritising things.

In the summit, there were four tracks of Panel Discussion sessions along with a live show case of the probable threat of using VPN (Virtual Private Networks) and the potential risk associated with the growing payments through RTGS. Followed by the Corporate presentation/ FireSide chat with VARINDIA and Experts speech.

The event kick-started with the welcome address by Dr. Deepak Kumar Sahu, Editor-in-chief- VARINDIA. Welcoming everyone, Deepak said, "The outbreak of Covid-19 posed life threatening challenges but our high speed 4G connectivity infrastructure has proved to be India's digital lifeline. Throughout 2020 the whole world worked online, studied online, worked online, received healthcare online, socialized online, played online simply put thrive online."

ENLIGHTENING ON VARIOUS FACTS RELATED TO THE CYBER SECURITY THE INDUSTRY LEADERS SAID:

TECHNOLOGY RELATED CRIMES WILL INCREASE EVERY DAY

LOKNATHBEHRA
IPS, Director General
Police, Government of Kerala

"Hi-tech crimes will increase as our way of living is very intimately connected to technology, whether it is Information Technology or BioTechnology. There will be an increase in the number of crimes which are committed either by using technology or the technical mind. As a police officer, I feel that technology related crimes or information related crimes will increase every day. We have a knowledge management system for training. We even teach the constables and sub-inspectors, who are directly recruited and those people who are sent for institute training."

AS PEOPLE ARE FORCED TO MOVE TO DIGITAL PLATFORMS THE GAP HAS COMPLETELY GONE

ANYESH ROY
IPS- DCP, Cyber Crime- Delhi Police

"The country is evolving in terms of usage of the internet and as well as devices which rely on the internet for communication. The devices gradually metamorphose into smaller things and becoming portable, more accessible on the move plus the number of applications used in these devices have gone manifold. Whatever gap that is remaining, has gone with the lockdown in March 2020. People who are reluctant, they are forced to move to digital platforms and in a way the gap has completely gone. We have actually made a quantum leap towards integrating our society to the digital platforms."

THE SURVIVAL OF THE BUSINESS DEPENDS ON MAINTAINING TRUST

DR. SANJAY BAHL
Director General- CERT

"Accelerating business transformation means accelerating change management strategy which can be defined as accelerating any shift or re-alignment or fundamental change in business operations. This acceleration is required as the business can survive and thrive in an environment, which is throwing new innovation driven opportunities as its response to shifting market demands while navigating the evolving regulatory complexities. The survival of the business is now dependent on maintaining trust in the services that it provides."

IN EVERY 11 SECONDS ONE COMPANY GLOBALLY BECOME VICTIM OF HIGH-TECH CRIME

DR. PAWAN DUGGAL
Expert in cyberlaw and e-commerce law- Supreme Court of India

"The Indian BFSI sector is neither safe nor good zone to be in, as this is now a fertile potential attack target. This shall be attacked by state and non-state actors.Globally, ransomware has become a big menace and challenge. Infact every 11 seconds, one company, anywhere in the world, becomes a victim of this high-tech crime. Government on the other hand has launched an online diploma for Law Enforcement agencies in terms of helping them in assisting in investigation of high-tech crimes"

UP POLICE'S DEDICATED APP HELPING PEOPLE TO FIGHT CYBER CRIMES

PROF. TRIVENI SINGH
IPS, UP POLICE

"Cyber-crime has increased during the pandemic in the fields of social media account, corporate sector, financial sectors and phishing attacks. We are facing an increase rate of child pornography cases in this period. Many people have committed suicide due to bank account fraud cases. There is also a major problem regarding fake accounts in Social media. We have a dedicated app for UP Police where people can lodge an FIR online."

CYBERCRIME IS THE FUTURE OF GEN-NEXT CRIMES

D SIVANANADAN
IPS- Ex Commissioner, Mumbai Police

"Since pandemic as people are jobless, property crime has gone up. Cyber-crime is the most important property crime, as in this crime, one does not have to visit the crime spot. Future crimes will be cyber related.Police is an integral part of society. They have to upgrade themselves- hardware and software. Not only officers, but even constables too have to be trained in cyber usage, and detection and prevention of crime, by using cyber instruments.

ONLINE TRANSACTIONS COME WITH A BIT OF DANGER

DR. HAROLD D'COSTA
CEO- IQSS

"Practically since last one year, there was no work for people, and even if there was any, it was done from home. And hence, the cyber security breaches have gone up exponentially. In today's circumstances and scenario, every bank account holder should question a bank about its cyber security policy, if they are followed by the bank and if they are examined by RBI. The RBI also in 2017 in cyber security practises has laid down specific rules and regulations, which seem good on a piece of paper but when it comes for implementation, it's a big shock. Corporative banks put the onus that nationalist bank is responsible to pay the money to them. This flashed as a heading on a certain channel. This has been in process from their side. Here, the nationalist bank is not at fault, as it has two security practices in place."

DATA HAS BECOME AN INTEGRAL PART OF EVERYONE'S LIFE

RAJSHEKHAR RAJAHARIA
Internet Security Researcher

"These days we see every single person using the internet. Be it farmer, sitting on the border, he talks about cyber security, and his personal data along with other things. These days one's data is vulnerable to cybercrime, or even fraud, hence cyber security is not just important for companies, but for individuals too.

We have to prevent financial data with much precaution as Whatsapp banking etc., are risky. As everything is now coming under eCommerce, as one shall hardly visit the store, he/she shall use the card instead. In that case one has to limit his card. Banks these days give such offer limits, but at times common man generally neglects it and falls victim to these traps."

CYBERSECURITY IS AS IMPORTANT AS PHYSICAL STRENGTH

TRISHNEET ARORA
Founder- TAC Security

"People are unaware about cyber security. They don't believe that their data can be stolen. Not large enterprises, even SME level or MSME level enterprises' data are at risk, as they become easy victims of cybercrime or cyber threat. They are unaware about digital assets that can be hacked, as they are unaware about any digital asset they are holding. Unless organizations are aware about the digital asset they are holding, only then they will be aware of cyber security".

EVERY ORGANIZATION MUST BE PRE-PREPARED FOR THE THREAT ATTACKS

BISWAJIT MOHAPATRA
Partner & Executive Director- Global Hybrid
Cloud Transformation Services- IBM

"Social media is becoming the best platform for the cyber criminals to conduct their criminal activities- be it identifying the data leakage, or phishing or even malware attacks; it is like a breeding ground for most of the hackers or cyber criminals. The first thing any organization has to do is to create a cyber security response intelligence plant- a living document that needs to be constantly, continuously and consistently monitored. Every organization needs to implement a security operation center- that will monitor any vulnerabilities and if any, is taken care of. Also, let's not forget ODR practice- Observe, Dictate & Remediate at a very faster pace. Hi-Tech crime may increase, but if one implements right platforms, right solutions to prevent those, then one can save their organization from big time crises."

4G CONNECTIVITY INFRASTRUCTURE HAS PROVED TO BE INDIA'S DIGITAL LIFELINE

DR. DEEPAK KUMAR SAHU
Editor-in-chief
VARINDIA

"The outbreak of Covid-19 posed life threatening challenges but our high speed 4G connectivity infrastructure has proved to be India's digital lifeline. Throughout 2020 the whole world worked online, studied online, worked online, received healthcare online, socialized online, played online simply put thrive online. I thank all the CIOs', CTO's, CISOs, the digital transformation leaders and the VARs of India for sharing their valuable inputs related to security journey. And I am here to share the vision of VARIndia on how India's digital future looks like. As we step into 4th industrial revolution, India has an opportunity not just to catch up with the leaders but to emerges as a global leader itself. Gone are the days of simple firewalls, antivirus being your sole security measures. From website intrusion, and malware propagation, malicious code, phishing, distribution denial of service attack, website defacements, unauthorized scanning and activities and ransomware data links- all these major threats have shown us the importance of high-tech cyber security measures in 2020. With the growth of a connected eco system upon which the vast majority of businesses rely will continue to face existing and emerging security threats in years to come. But by designing and enforcing a vulnerability management program companies can identify and mitigate these accordingly. The year 2021 is very much significant for all the industries as it is a drone of the digital age. Since everything is happening online and digitally, the need for cyber security is now greater than ever. Therefore, in order to sustain business online, and create a safe workflow, cyber security solutions are of great importance."

SPAM AND PHISHING ATTACKS WILL CONTINUE TO GROW IN 2021

NITIN DUBEY
Senior PreSales Manager,
South Asia- Kaspersky

"In this pandemic time, we have seen cyber threats increasing multi fold and major reasons for that are human error, unpatched vulnerabilities, accessible RDP and weak passwords. When we talk about human errors, without surprises spam and phishing is the number one attack factor. We have seen an increase and the trend will continue in 2021. The pandemic has pushed us to work from home and we have seen a significant increase in RDP attacks in comparison to earlier times. Ransomware is the fourth major attack factor and becoming a serious threat to all the organizations."

INGRAM MICRO HELPS ORGANIZATIONS DEPLOY ROBUST AND RELIABLE SOLUTIONS

NAVNEET SINGH BINDRA
VP & Country Chief Executive,
Ingram Micro India

"Ingram Micro security provides access to leading cyber security OEMs along with a comprehensive set of services that help organizations deploy robust and reliable solutions that are well suited for their needs. Our portfolio of security vendors covers domains such as identity management, threat management, data protection, risk assessment etc. We offer a diverse set of security vendors ranging from industry leaders to innovative ISPs that provide every kind of security that businesses today may need."

DATA AND PEOPLE WITH THEIR EXPERIENCES SHOULD BE SAFEGUARDED WITH SECURITY

SUDEEP DAS
Technical Sales Leader, IBM Security

"I will focus on the two primary aspects that I want to safeguard, first is data and the second is people and their experiences with security. The identity and how they are accessing the data and the applications. These two things are going to sit on the ecosystem of different technologies and different infrastructure. When I put this data security in identity access management in an open security ecosystem and manage the threats against this then we have sort of starting blocks like threat management, data security, identity access management and an open platform where each of these elements can talk to each other and leverage each other's things."

POST LOCKDOWN ENTERPRISES LOOKED AT BUSINESS RESILIENCE AS THE PRIORITY

R. VENKATESH
President, Enterprise Business Group, Redington India

"As you all know we are in a forced lockdown scenario, enterprises had to prioritize business continuity. Work from anywhere and work from home became the model, there was no other option. That is when one level of security evolved and organizations had to think about it and post that slowly things got better. Post lockdown enterprises looked at business resilience as the priority. That is why they had to adopt hybrid cloud, and started moving applications to cloud."

THERE IS AN EXPONENTIAL INCREASE IN THE NUMBER OF ATTACKS

RADHESH WALWADKAR
Manager - Systems Engineering (India & SAARC)- Fortinet

"As an endpoint security customer, you might be coming across various terminologies like next-generation anti-virus, EDR, XDR. There is an exponential increase in the number of attacks which are becoming successful on the endpoint from 3.2 million to 1 billion in a very short period of time. This raises a question about whatever endpoint security mechanism I am using today whether it is really effective or do I need to change that certain endpoint security mechanism."

THE RISE OF CYBER-ATTACK TARGETING THE DATA AND CRITICAL INFRASTRUCTURE OF NATIONS IS UNDENIABLE

MALAY UPADHYAY
Sophos Sales Engineer-Sophos India

"Much has been talked about cyber security and the threat landscape, as we know that the threats are getting more and more sophisticated in nature and on rise than ever before. There is a strong need to automate the defence mechanism. The rise of cyber-attack targeting the data and critical infrastructure of nations is undeniable. With no signs of slowing down from state-sponsored hackers to activists to criminal enterprises groups are leveraging the power of automation to deploy malware with speed and scale given the automated nature of many of the attacks."

CYBER-CRIME IS MARCHING WITH TIME AND SPEED

SUNIL SHARMA
Managing Director(Sales)- Sophos

"If you look at data, cybercrime has increased but today the crime which has increased is where people are targeted. There are sophisticated attacks which are happening to the larger enterprises' data account. There they know what the criminals want to do and at the same time if you look over all in terms of numbers and data, the cybercrime is also marching with at the same time and same speed. It has actually not increased. As people are working from their homes and become more vulnerable, hence the crime is seen more."

THE VALUE OF VISIBILITY COMES FROM INTELLIGENCE

GURUPRAKASHRAYASA
Country Head of Sales- NSS INDIA- Keysight

"The acquisition of Ixia strengthens Keysight's position in Network visibility, network testing and network security as well as the visibility for cloud services in traditional and software defined.

Network visibility is a fancy way to say make it easy for the security and marketing team to find issues which could be critical cyber security threats and fix it. The value of visibility comes from intelligence, not just data but understanding what is happening in the network."

THE FASTER TO DETECT A BREACH; THE LESS THE DAMAGE WILL BE TAKEN

HO YEOW SIN
Technical Lead in Southeast Asia, Hillstone Networks

"Enterprise security has been focusing on prevention. Security defences like firewall, IPS etc are always the parameter of trying to keep the bad guys out. Parameter defences are still useful, but interestingly there are ways to get around the parameter because of technology changes. Needless to say, there are also internal attackers who do not even need to cross a parameter."

INDIAN MARKET WILL BE THE NEXT GROWTH FOR HILLSTONE

WILL RONG
Regional Sales Director, SEA, Hillstone Networks

"Hillstone Networks is funded by industry veterans to deliver innovative proven & effective narrow security solutions to more than 18, 00 customer worldwide, including 4500 enterprises financial and educational organizations, government and service providers.

In 2021 we are really focused on this region especially in Indian markets. We have put a lot of resources including sales and technical team and also our partner in Indian market. I do believe Indian market will be the next growth for our company. I also believe all of you can benefit from Network security solutions."

THE PANEL DISCUSSION SESSIONS WITH THE LEADERS FROM THE BFSI (BANKING, FINANCIAL SERVICES AND INSURANCE SECTOR) WERE VERY INFORMATIONAL AND IMPACTFUL. THE DISCUSSION IN THE BFSI IS IMPORTANT AS THE MAJOR DRIVING FORCE FOR THE GROWTH OF THE IT SECURITY MARKET IN INDIA. THE PANELLISTS SAID:

CYBER & DATA SECURITY SUMMIT 2021

VARINDIA

PANEL DISCUSSION (SESSION- I)

Technology leaders from the BFSI sector

TOPIC

BFSI HAVE BEEN THE MAJOR DRIVING FACTORS FOR THE GROWTH OF THE IT SECURITY MARKET IN INDIA

Milind Varerkar
CIO
Saraswat Bank

Upkar Singh
Director
IT FIS Global

Pawan Chawla
CISO
Future Generali India Life Insurance

Kapil Mehrotra
Group CTO
National Capital Management

Kapil Madaan
CISO
Spark Minda

Sindhu Bhaskar
Co-Chairman
EST Group

60-70% ORGANIZATIONS ARE NOT READY TO FACE THE CHALLENGES

KAPIL MEHROTRA
Group CTO- National Capital Management Services

"Nowadays vectors are getting stronger day by day but most of the organizations are not ready with that change. In terms of percentage 60-70% organizations are not ready. This is one of the big risks. The people are not fully aware of it till now. Looking at these two major challenges we have to take care of the right implementation part and look for the right solution."

INDIA NEVER HAD THE CULTURE TO WORK FROM HOME

PAWAN CHAWLA,
CISO-Future Generali India Life Insurance

"Ever since the COVID-19 started, it has changed many things. One, it has changed the way we look at cyber security, secondly the way it does the business, third the way the threat factor used to perform their task. India never had the culture to work from home, with COVID-19 things have changed drastically. Every organisation today has this culture of Work from Home. They have adopted the WFH culture, although they were not ready in the initial few days."

THE PANDEMIC HAS INCREASED THE ATTACKS

MILIND VAREKARM
CIO- Saraswat Bank

"We need to ensure the safety of end customers. So, when we are taking care of the base at the infrastructure level one more challenge remains is to make each and every employee aware about their bank's security perspective. During the pandemic it has been noticed that the attacks have been increased. We also need to ensure that the customers are aware of taking care of their own banking transactions."

CYBER-ATTACKS HAVE NOT COME OUT ALL OF A SUDDEN

DR. SINDHU BHASKAR
Co-Chairman & Founder-EST Group

"We were in the digital world but neglected it from the beginning. We had the computerized environment but did not take full care of all the malwares and attacks. We were trying to be on the expansion mode rather than safeguarding our technologies. But now the focus has come due to the pandemic. The cyber-attacks were present all of these years; it is not that these have come out all of a sudden."

CISOS FILL THE GAP BETWEEN BUSINESS, TECHNOLOGY AND SECURITY

KAPIL MADAAN
CISO- Spark Minda

"Cyber security has continued to take the centre stage. India is the second most ideal country for ransomware. It increased approximately 40-50 % in 2020 compared to last year. It is important that we start taking cyber security seriously. It completely depends on CISO's strategy and preparedness to handle newer security risks, CISOs fill the gap between business, technology and security. We should come with an approach of a single click awareness solution."

THE SECURITY URBANIZATION IS PARAMOUNT OF IMPORTANCE

UPKAR SINGH
Director IT- FIS GLOBAL

"Security for us is basically two-fold, internal and external. It is very critical for any service organization like us. The security has to be built on multiple levels, not only as the batch processing of the code we build. Security urbanization is of paramount importance from the beginning. From physical security, network security or software security or endpoint security is of much more importance."

FUTURE DIGITAL ENTERPRISE WILL ONLY DEPEND ON COMPANIES WITH GOOD DIGITAL FOOTPRINT

PARNA GHOSH

Vice President & Group CIO-UNO Minda Group

"Cyber security challenges are not only impacting the enterprises within their boundaries; it is also impacting the employees or individuals who are working in the enterprises. It is also impacting the individual's devices like mobile phones or laptops and other devices and applications. It is spreading across and covering both the employees and the enterprise. In our organization we are doing a lot of reforms as we have understood one thing, future digital enterprise will only depend on companies who are really good and strong in processes with good digital footprint."

SECURITY SHOULD BE THE PRIME FOCUS NOW

SUBROTO K PANDA

CIO-ANAND & ANAND

"The pandemic has actually helped in development and adopting the security measures. Prior to pandemic our organization was completely offline but it became online all of a sudden. Security should be the prime focus now with enterprises getting into work from anywhere or work from any device and be always available."

THE PRIVACY OF THE USERS AND THE DATA SECURITY SHOULD BE MAINTAINED

RISHI MEHTA

Technology Evangelist- Silicon Valley (USA)

"The one big challenge is how much data should be used. As part of cyber security, you need to protect, but you need to use the data also and those lines have to be drawn somewhere on how you use the customer's data or the company data or the supplier's data. As you build the regulations to protect the privacy of the users and the data security, the way should be that you are not only protecting the assets around the data and the users but at the same time you are not stifling the innovation."

IF A PERSON THINKS HE IS 100% SECURED THEN HE IS REALLY A FOOL

BHARAT B ANAND

Group IT Head & Security- EC Council

"There is nothing called inside in security whether it is physical or cyber. There is no term called full proof security, if a person thinks he is 100% secured then he is really a fool. We always say it is not about if, it is always about when. The concept we should always remember is to keep working, keep testing hypotheses continuously to figure out the gaps and work on them to shore up our fences so that we are better placed."

DIGITALIZATION HAS A SIGNIFICANT IMPACT ON BUSINESS IN TERMS OF TRANSFORMATION

CHANDRA MOULI

CIO & CTO-Sankara Nethalaya

"Looking at my own experience in the financial services industry, I can say we have seen a lot of digital transformation now the way the business is going. Every risk that you see with all the digital initiatives that are coming around is also adding an element of risk. There is a quantum change particularly with all the digital play coming into the picture. Digitalization has a significant impact on business in terms of transformation but equally adding to the issues around another compliance and security particularly."

CYBER SECURITY IS THE KEY COMPONENT FOR ANY BUSINESS

DR. VINEET BANSAL

CIO-Greenpanel Industries

"Cyber security is very important when we talk about the digital transformation which is happening today in all industries, specifically in the manufacturing sector. Cyber security is the key component as we have seen during the Covid time. Most of our resources were working from home and there was a big challenge of managing cyber security."

THE NEXT SESSION FOCUSES ON HOW THE CORPORATE AND VARS ARE GEARED TO OFFER THE SECURITY AND CYBER SECURITY AS THEIR SOLUTION OFFERINGS.

PHARMA BREACHES CAN BE TERMED AS MOST CRITICAL

B. RAJARAMAN
Manager – Technical, Raksha Technologies

"Work from Home was new to many of the organizations, as they have embraced this. Though it is a common term used in the IT landscape, it comes along with challenges. Many IT organizations are struggling to implement the entire compliance requirements. On the other hand, we can see many breaches happening. Pharma breaches can be termed as the critical ones. It is clearly seen though we have security problems, the infrastructure is growing protected, and there are a lot of gaps that every organization has to fill yet. There are a lot of vulnerabilities seen to the known software which are used by the organization to run their day-to-day operations. And these softwares are used in the industry for many years."

The summit continues with the next panel discussion session. In this session we had various take-aways from the Cyber Security consultants, Cyber law makers and the Influencers in the Industry. The topic of the discussion was " Sophisticated cyber criminals adopting Hi-tech cyberattack techniques to target end-users".

CORPORATES HAVE TO BOTHER FOR CYBER SECURITY IN GENERAL

DR.KARNIKA SETH
Founder-Seth Associates

"Data is huge, and data is the new oil. So we are worried about Cyber security not just from the point of view from how we protect just non personal data of people, which could be of businesses- not only their consumers, contacts, but also about the data of their citizens. Corporates need to worry on all fronts- legal, technical and cyberspace in general."

CYBER SECURITY IS NOT JUST AN IT GAME, BUT MUCH DIFFERENT!

ANUJ AGARWAL
Chairman- CybrotechDigiventure

"In terms of Corporate, the threat is from inside and outside- mostly from outside. The risk is mostly the management people are not involving themselves into cyber security and they are leaving it on their IT people as they are good at delivering IT solutions. Cyber security is totally a different ball game."

INSIDE HACKER IS MOST DANGEROUS THAN THE OUTSIDE HACKER

HAROLD D'COSTA
President-Cyber Security Corporation

"There are two types of hackers- Inside hacker and outside hacker. If an inside hacker does not provide any information to an outside entity, then there will be very less element of any unauthorised hacking taking place.As far as outside hackers are concerned, they can commit any attacks like ransomware attack, modifying the part of your folders... But mainly corporate problems are when the inside person provides information to the outside entity for the crime to be taken."

ORGANIZATIONS HAVE TO BE MUCH AWARE ABOUT CYBER SECURITY

SANDEEP SENGUPTA
CEO- ISOAH

"Lack of awareness is the most important point brought into awareness that starts from the top management. Most of the top management are clueless about the risk and the type of control. Thinking from a country point of view, the PSU, power grid, stock market, banks are the biggest vulnerable points as they are still using a lot of back-dated technology. If there is war breaking out, we will be in serious trouble. Because small time hackers etc cannot do much damage, but if the Power sector becomes a victim, it becomes a national security issue."

CYBER SECURITY HAS BECOME A HOT TOPIC THESE DAYS

HARNATH BABU
CIO-KPMG India

"Cyber security is becoming one of the top concerns in most of the organisations as we are dealing with data.With the advancement of technology, the more opportunities (hacking) that have been created, we are making it more vulnerable from a data security point of view."

CYBER SECURITY IS NOT AS EASY AS FEW PEOPLE THINK

SUBHOSHAN MUKHERJEE
Founder-Prime Info Serve

"Any enterprises across the globe are trying to prevent the attack. Attack cannot be prevented. Many breaches across the globe, starting from Equifax to Sony, the moment attack takes place. At this point of time Cyber security is not as easy as few people think. As we are talking of multifactor attack, signature less attack, hence cyber security has to be treated like a family. To handle ransomware attacks, check on every possible threat."

THE NEXT PANEL DISCUSSION WAS ON "BUSINESS RESILIENCE WITH DIGITAL CAPABILITIES IS A BARE NECESSITY FOR VAR'S TO SURVIVE".

VARINDIA

BUSINESS RESILIENCE WITH DIGITAL CAPABILITIES BECOMING A NECESSITY FOR VARS TO SURVIVE.

To be live on

Cyber & Data Security Summit

19th, Feb 2021

LIVE ON

www.varindia.com

VARINDIA CYBER & DATA SECURITY SUMMIT 2021

CYBER & DATA Security Summit 2021

SESSION - IV

MR. RANJAN CHOPRA
CEO & MD
TEAM COMPUTERS

MR. VISHAL BINDRA
CEO
ACPL SYSTEMS

MR. KRISHNARAJ SHARI
DIRECTOR & CEO
IVALUE

MS. RAMANDEEP SINGH
DIRECTOR
QOS

MS. MANASI SAHA
FOUNDER
MACAW INFOTECH

MR. AJAY BHAYANI
DIRECTOR
AMBISURE TECHNOLOGIES

PROACTIVENESS IS THE BEST SOLUTION FOR RANSOMWARE

KRISHNARAJ SHARMA
Director &CEO-IVALUE Info Solutions

"Ransomware is a very reactive problem to happen. Proactiveness is the best solution for ransomware. As long as we protect our data, we can minimise the chances of ransomware. Understand first which data is critical to the organization. Attackers very well know what data is critical for the organization. It is important for the organization to identify the critical data before the hacker does. In a large network it is necessary to identify where the critical data is, especially when you have customer data, customer asset data etc, and also identify the people handling it."

RANSOMWARE ATTACK CAN ONLY BE PREVENTED IF ALL SECURITY UNITS ARE TOGETHER

N K MEHTA
M.D.& CEO-Secure Network Solutions

"Ransomware is still coming to traditional channels- like email, web and the end point. According to Verizon Security Reports, 90% is delivered by email. Earlier, the organization used to have a point approach- the best of parameter security or best of the end point from different vendors from different partners.

Today, we need to look at a solution which integrates all various channels into one. One may have parameter security or email security- but if neither of them works together, we are surely opening the doors for smart ransomware attackers to get into the system. But if all the security work together is like a tightly closed unit, with a centralized view, then there is a chance to protect against ransomware attack".

RANSOMWARE IS CERTAINLY ONE OF THE LARGEST THREATS FACED BY CORPORATES

VISHAL BINDRA
CEO-ACPL Systems

"Ransomware is one of the largest threats faced by corporations. The biggest testimony is that added more than 500 thousand endpoints, more than EDR in the last 4 months itself. It is true that endpoint security is not going to be that strong, but with COVID coming in, it has really changed everything.

After doing such a large implementation, we can realize one thing, we are buying tools which will give us a lot of indicators of compromise, what is happening, and they will give us a lot of indications. We are deliberately looking at data coming to us from all of these devices. We have created tools to do that."

RANSOMWARE ATTACKS ARE THESE DAYS HAPPENING CONTINUOUSLY

AJAY BHAYANI
Director-Ambisure Technologies

"Ransomware has been into the picture since decades. And here the most important thing is it is happening relevantly, but what has really changed is the organizations had really prepared themselves to fight against ransomware in the pre COVID scenario where everything was inside their environment.

And that's what has changed. The scenarios to protect oneself from ransomware have completely changed. If one really wants to protect themselves from such scenarios, backup is the way."

TO TAKE THE CHALLENGES ONE SHOULD BE TECHNICALLY EQUIPPED

MANASI SAHA
Founder-Macaws Infotech

"For last 20 years Macaws has been in the cyber security business. I started the journey with network security, went to infrastructure security and now into cyber security.

As per Macaws is concerned, we believe in three things first, we have to take challenges. Secondly, we have to be equipped enough technically and third, customers have to be with me. I rely into innovation and transformation."

RANSOMWARE COMES WITH STAGES TO BE DEALT WITH

RAMANDEEP SINGH
Director-QOS

"The most important thing about Ransomware is the stage it comes to the surface or known to the organisation which is trying to deal with it- that defines with protection scale it should be defined. Every small or big organization is well aware about ransomware. Ransomware is one such problem, and is known in the common man's space. There is protection, prevention solutions available, to commensurate to the risk an organisation has. But it is all about the managed services, the subsequent services layers that have been built by the virtue of the inside team, or by the outsource team or sub contract team."

SECURITY IS A MUCH-SPECIALISED THING

RANJAN CHOPRA
CEO & MD-Team Computers

"During security operations, when close monitoring is being done, expert services are being provided. A massive opportunity has been seen on the application side. As we were running managed services for 24*7 remote operation for a lot of customers, we have now added on security operations as well. I see this as a high growth area. Security is a much-specialised thing. Hence, we use both approaches- build and buy. We build some expertise internally and we will buy and partner with organizations on the panel, so that our customers get the best. Security threats are all over- email, parameter security, application security; all areas are very vulnerable."

NEXT ON THE AGENDA WAS TO PRESENT THE MOST AWAITED AWARDS CEREMONY BASED ON HOW THE CORPORATES HAVE PERFORMED IN VARIOUS CYBER SECURITY SOLUTIONS IN THE INDIAN MARKET.

Award winners in the 5th Cyber Security Summit 2021

Best Identity & Access Management (IAM) solution	IBM India Pvt. Ltd.
Best Next Generation Firewall	Fortinet Technologies India Pvt. Ltd.
Best DLP solution provider	Broadcom India Pvt. Ltd.
Best DDoS protection company	Radware India Pvt. Ltd.
Best cloud security company	Cisco System India Pvt. Ltd.
Best company into malware protection	Sophos Technologies Pvt. Ltd.
Best EDR solutions	Crowdstrike India Pvt. Ltd.
Best company into email security	Checkpoint Software Technologies
Best Internet security	Kaspersky
Best Cyber security company of the year (On Cloud)	Akamai Technologies
Best Cyber security company of the year (On Hybrid)	IBM India Pvt. Ltd.

NEXT WAS THE MOST INTERESTING SESSION ON HOW THE "VIRTUAL PRIVATE NETWORK" (VPN) CAN ALSO BE HACKED.

AREAS OF ATTACKS ARE REDUCED

PRASAD T
CISO- INSTASAFE

"No company can overnight become highly secured. In today's world every company is using VPNs and firewalls to protect their parameter of infrastructure. It is the time to move on from VPN to Zero trust, because VPN technology has evolved over the time and Zero trust makes sure that these infrastructure and elements of it, like devices and applications are completely hidden. Areas of attacks are reduced when it comes to hacking an organization. It is a journey, not an easy game. Sometimes companies take up upto a year. We have to mature; we have to ensure that all our infrastructures are protected. Zero trust is a way to go, is all I would say."

IT IS TIME TO MOVE FROM VPNS TO ZERO TRUST

Next in the Fireside chat was
SANDIP PANDA
Founder- Instasafe

"Through this session the CIOs, CISOs and risk management professionals got an opportunity to understand what are the key vulnerabilities of the existing VPNs and how they could be exploited with readily available scripts on tools. Known vulnerabilities were always there. It is the time to move from VPNs to zero trust."

AI HAS BEEN PARAMOUNT IN BUILDING AUTOMATED SECURITY SYSTEMS

S MOHINI RATNA
Editor-VARINDIA

"With AI being introduced across the industry and most of the sectors are geared for the challenges and opportunities. The technology comes with a combination of machine learning that has brought tremendous changes in cybersecurity. AI has been paramount in building automated security systems, natural language processing, face detection, and automatic threat detection. AI-enabled threat detection systems can predict new attacks and notify admins for any data breach instantly, making it the next cyber security trend in 2021."