ITPV

Connecting with Solution Provider in
EMERGING MARKET

Vol XII | Issue 1 | May 2022 | Pages 32

■ Northern ■ Eastern ■ Maharashtra ■ Gujarat ■ MP & Chattisgarh ■ North East ■ Southern ■ UP & Uttarakhand ■ Bihar & Jharkhand

Building Cyber Resilience with Innovation

May '22 Edition

TECHPLUS MEDIA

Looking for a compact, efficient and robust UPS? Look no further!

VERTIV.

Presenting

Liebert ITA2 30kVA

A fully digital, highly reliable, double-conversion UPS solution.

Its cutting-edge design enables seamless integration into your current system, or various other ecosystems. And it's tailored for global deployment in a low carbon, compact footprint. The ITA2 is the ultimate level of engineering and dynamics from Vertiv. So, you can deploy this innovative, next-gen and extract great performance at low costs. Adding up to peace of mind. If you're looking to power your infrastructure, or upgrade your already protected systems, the ITA2 is a great addition to your support backup.

Talk to us today!

Explore solutions at Vertiv.com/en-in
Call Tollfree : 1-800-2096070
E-mail : marketing.india@vertiv.com

Corporate Office : Plot C-20, Rd No.19, Wagle Ind Estate, Thane (W), 400604. India

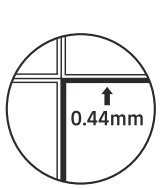
SCAN CODE
TO KNOW MORE

SAMSUNG

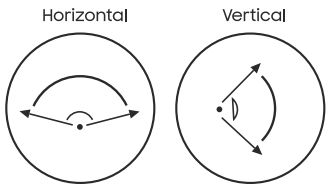
Seamless video walls with razor-thin bezels

Make a deeper visual impact with Samsung's Video Wall. Its powerful picture enhancement technology delivers robust, seamless, and vivid pictures for every business need.

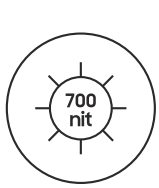
Striking features



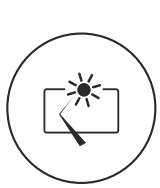
Razor narrow bezel



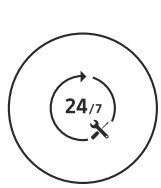
Wide viewing angle



High brightness



Non-glare



24/7 operation

For more information, call +919717194965 or email ceb2bsales@samsung.com

T&C apply. Image simulated, for representational purposes only.

Cheil-11484/22

CONTENT

Building Cyber Resilience with Innovation

Recent global events have shown that innovation is essential for enterprises to survive and flourish. But accelerating digital innovation brings new complexity and risk. In the current scenario, let's analyze how organizations can anticipate new cyber-security threats, deal with disruptive technologies and build resilience in a world where anything seems possible

Amit Singh

In the aftermath of the pandemic, as boundaries between remote workplaces and offices have eroded, cyber attackers are discovering new ways to intrude and misuse sensitive data, both personal and corporate. Concurrently, while automation and digitization have presented infinite growth opportunities, they have also widened the technological surface for cyber-attackers to exploit.

More than 11.5 lakh incidents of cyber-attacks were tracked and reported to India's Computer Emergency Response Team (CERT-In) in 2021. According to official estimates, ransomware attacks have increased by 120 percent in India. Power companies, oil and gas majors, telecom vendors, restaurant chains and even diagnostic labs have been victims of cyber-attacks.

Pandemic silver lining

Every crisis has a silver lining and for the pandemic, it has been the accelerated adoption of digital solutions across enterprises and governments. Decade's worth of digital transformation has taken place in the last two years and India's technology industry has emerged as the preferred digital solutions partner with cybersecurity as a key growth vertical. Cybersecurity is now a boardroom agenda and offers tremendous opportunities for India's tech industry to build innovative solutions and services.

This boardroom focus has enabled India's cyber security industry to nearly double in size amid the pandemic, with revenues from cyber security products and services growing from $5.04 billion in 2019 to $9.85 billion in 2021, according to Data Security Council of India report. The services industry grew from $4.3 billion in 2019 to $8.48 billion in 2021 at a CAGR of 40.33 percent. The product industry grew from $740 million in 2019 to reach $1.37 billion in 2021 at a CAGR of 36.49 percent.

At the same time, India's cyber security workforce swelled from 110,000 employees in 2019 to 218,000 in 2021 even as talent shortages remain.India's cyber security startup and product industry also saw robust growth, raking in revenues worth $1.37 billion.

"Global CEOs and CFOs have highlighted that cyber security is the largest factor which could halt the growth and profitability of the organizations. As per our global survey, two-third of the global CEOs say that robust cyber security makes them feel stronger, confident, and enable them exploit more power of digital."

Akhilesh Tuteja
Global Leader - Cyber Security, KPMG

Biggest factor to halt organizational growth, profitability

Cyber security has remained among the top five factors which impact the growth for the CEOs around the world shares AkhileshTuteja, Global Leader - Cyber Security, KPMG. "Global CEOs and CFOs have highlighted that cyber security is the largest factor which could halt the growth and profitability of the organizations. As per our global survey, two-third of the global CEOs say that robust cyber security makes them feel stronger, confident, and enable them exploit more power of digital."

He further underlined that CISOs are not just reducing risk but are actually creating humongous value for the organizations. "In fact, the role of CISO is getting quite hard due to scarcity of skilled resources and cyber security being highly technical job requiring deep expertise.

"With lots of exclusion clauses, complications in claims, and dismal claim settlement ratio, cyber insurance is not a great idea for risk aversion. Moreover, paying ransom could be a disaster as the organization may turn out to be an excellent value proposition and lucrative customer for cyber attackers with repeated invasions."

Steven Sim Kok Leong
President, ISACA Singapore Chapter & Chair, OT-ISAC Executive Committee

"We could look at it from the perspective of importance of data that need to be protected. So we may argue that the spending on security will be justified by the value of the data that we may lose or may be jeopardized."

Dr. Rizwan Khan
CFO-CIO, Panoval Asia

Indeed, there is large demand and supply gap in skilled resources in cyber security, which leads to overburden and stress among the security personnel. Hence, CISOs and security experts deserve high level of respect."

With several recent incidents of data breach, India's cyber security market so far proves the robust demand. But is the country ready to meet this demand and is it preparing a cyber-security workforce for the unforeseen cyber future? Around 3.5 million jobs in the cyber security space was

estimated to be unfilled by the end of 2021.

Driving C-suite and board agenda

Setting the tone for the board room agenda on how to get the 'buy-in' from the CEO and the board to invest in the resources required for a robust cyber security, Steven SimKok Leong, President, ISACA Singapore Chapter & Chair, OT-ISAC Executive Committee underlines that boards need to understand the limitations of paying ransom and using cyber insurance as means of risk transfer. "With lots of exclusion clauses, complications in claims, and dismal claim settlement ratio, cyber insurance is not a great idea for risk aversion. Moreover, paying ransom could be a disaster as the organization may turn out to be an excellent value proposition and lucrative customer for cyber attackers with repeated invasions. Further, decryption tools offered in exchange of ransom usually turn out to be sub-optimal. Hence, robust cyber security governance and disaster recovery strategy are still the preferred risk-driven approach."

He adds that there is a need to invest heavily in operational and business resilience, business continuity, incident management and recovery measures. "CISOs need to discuss the business impact in terms of revenue loss, reputation loss, and regulatory fines that follow after the security breach. Above all, we need to assess the competitive advantage which comes as we showcase resilient-by-design architecture to the potential customers. Digital trust is crucial in the current scenario."

Elaborating on how enterprises can strike a balance between financial viability of security spending and having the optimum security infrastructure, Dr. Rizwan Khan, CFO-CIO, Panoval Asia mentions that security starts from top of the pyramid. "Top management must be aware of the significance and importance of cyber security. In addition, managers must be trained to respond to security incidents and most importantly, employees including team working on data must be sensitized, trained and be aware of whom to contact in case of any incident."

He further underlined that the challenge CISOs face is to justify the RoI in security spending. "We could look at it from the perspective of importance of data that need to be protected. So we may argue that the spending on security will be justified by the value of the data that we may lose or may be jeopardized."

"Attackers are always one step ahead. They are coming up with newer ways of intrusion which pulls the security teams into vicious cycle of attack and protection. If we truly want to defend against the new types of threats, we need to completely and drastically change the way we think."

Erez Kaplan,
Founder & CTO, Cyber 2.0

Disruptive Deep Tech to Protect from Advance Cyber Threats

The security battle is getting intense by the day. Attackers are now state sponsored and leverage on emerging technologies like AI and automation. "Attackers are always one step ahead. They are coming up with newer ways of intrusion which pulls the security teams into vicious cycle of attack

and protection. If we truly want to defend against the new types of threats, we need to completely and drastically change the way we think," saysErez Kaplan, Founder & CTO, Cyber 2.0.

He adds that chaos mathematics could be the way out. "Let's take our body for example. Our white blood cells and antibodies learn and act against the viruses and bacteria. However, viruses mutate and bypass our protection shield. If we put chaos mathematics on the communication between the cells, we will be able to block the communication between cells as the first cell gets infected. The attackers will be unable to bypass because the chaos mathematics is not crackable."

"The need is to understand why do people adopt risky behaviors and try to bypass security policies. If we get into the root-cause analysis, we identify that employees engage in risky behavior for their convenience, which is more important for them as compared to the security controls."

Mohit Gupta
Group CISO, Motherson Group

"We have seen fair bit of cyber-attacks on IT and OT systems as the threat vectors are getting more sophisticated. In this perspective, a relook at zero trust framework is necessary to bring in the security control to protect the convergence of IT and OT."

Akshay Garkel
Partner & Leader, Cyber, Grant Thornton Bharat

Endpoint Security:

Security from Home to the Enterprise

According to market estimates, over 36 percent of the employees find ways to bypass organizational security policies. "The need is to understand why do

people adopt risky behaviors and try to bypass security policies. If we get into the root-cause analysis, we identify that employees engage in risky behavior for their convenience, which is more important for them as compared to the security controls," shares Mohit Gupta, Group CISO, Motherson Group.

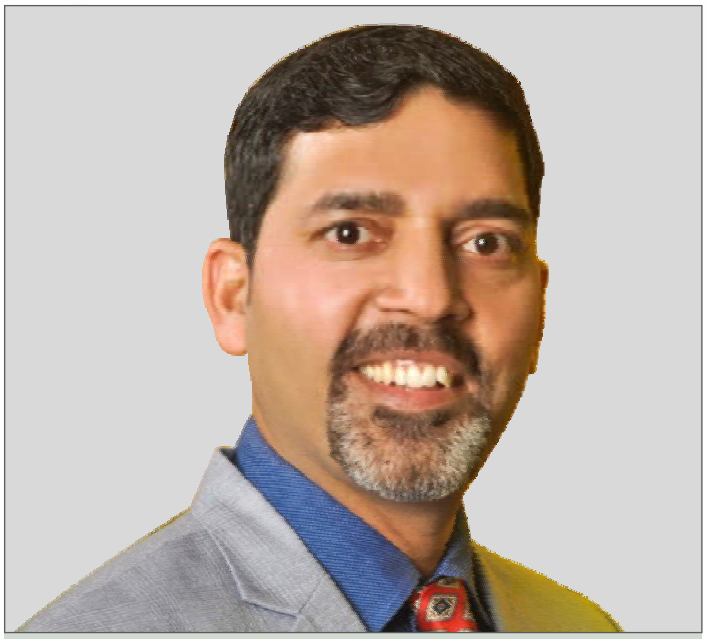
Hence, it is important to adopt technology and cyber security controls, but it is more crucial to evaluate and implement technology in such a way that strikes the right balance between convenience and security controls. "Picking a right technology is just one aspect of it. But how effectively, efficiently and smartly we implement the technology is something which is of utmost importance," Gupta adds.

He further highlights that emerging cyber security solutions are certainly important, however, it is crucial to focus on four core principle of cyber security to strengthen our cyber security posture. "The first principle is security by default, which is a cultural change to incorporate security in the solution planning itself. The second is defense in depth. The third principle is that the solution or technology that we adapt should be scalable and agile. And the last important core principle is resilience by design. It is important how we position the business to elevate the brand equity if something goes wrong, and gain and sustain the stakeholder's confidence. I guess that is where the answer towards cyber resiliency lies."

OT & IT Convergence: Security with Zero Trust

Most OT systems have been designed with very little consideration for security. With increased cyber risk in this new digital transformation era, any approach to bridge the IT and OT divide is mission-critical for enterprise security. While a 'zero-trust' approach has proved to be successful for most organizations in an IT environment, how does it work in an OT setup?

"Organizations which are using Operational Technology extensively have seen value in terms of converging both OT and IT together to fuel the mass digitalization wave. We have seen that IT systems support data-centric computing on the other hand OT systems help in monitoring and controlling device performance. However, we have seen fair bit of cyber-attacks on IT and OT systems as the threat vectors are getting more sophisticated. In this perspective, a relook at zero trust framework is necessary to bring in the security control to protect the convergence of IT and OT," states AkshayGarkel, Partner & Leader, Cyber, Grant Thornton Bharat.



> **"Organizations must strengthen their zero trust approach by taking little steps into that journey. Zero trust is a multi-year project which is driven by cultural changes in the organization. Further, we need to ensure an air gap between IT and OT architecture."**
>
> **Ambarish Kumar Singh**
> CISO, Godrej & Boyce

The way IT systems have grown could not be seen in the OT systems, which are mostly running on legacy operating systems. In addition, all the policies designed for the IT systems could not be applied to OT systems which shortens the visibility. "While businesses are rapidly driving digital transformation initiatives, they need to ensure the cyber security is integral part of the

journey. Most importantly, organizations must strengthen their zero trust approach by taking little steps into that journey. Zero trust is a multi-year project which is driven by cultural changes in the organization. Further, we need to ensure an air gap between IT and OT architecture," highlights Ambarish Kumar Singh, CISO, Godrej& Boyce.

Col (Dr.) Inderjeet Singh, Chief Cyber Security Officer, VaraTechnology adds that almost 85 percent of the traffic is not monitored by the firewalls and other security appliances. OT systems are quite difficult to secure as the air gaps are difficult to maintain. Further, IoT devices are connected to cloud which increases the vulnerabilities.

"Almost 85 percent of the traffic is not monitored by the firewalls and other security appliances. OT systems are quite difficult to secure as the air gaps are difficult to maintain."

Col (Dr.) Inderjeet Singh
Chief Cyber Security Officer, VaraTechnology

"We need to be capable of expanding security protection across multiple computing devices, containerized environments independent of underlying infrastructure. In addition, we need to have complete visibility through users, devices, components and workloads across environments."

NitinParashar
Senior Manager, Security and Compliance, Jio Platforms

Citing an example of cyber security controls in connected cars and smart manufacturing processes, he says that connected cars and driver-less cars have over 7200 embedded micro-controllers running millions of ports as all the controls are controlled by hundreds of sensors. To make it more interactive they have vehicle to vehicle communication and vehicle to infrastructure

communication, which are highly vulnerable. Hence, complete understanding of the attack surface is critical.

"Lots of auditing and privacy controls are to be built in to check any vulnerability. In fact, the car has to be treated as the moving data center, which has to have restricted access," adds Singh.

Highlighting the process and mindset changes, NitinParashar, Senior Manager, Security and Compliance, Jio Platforms reminds that zero trust is all about a mindset and process that we need to inculcate to prevent data breaches and contain lateral movement using application micro segmentation. "We need to be capable of expanding security protection across multiple computing devices, containerized environments independent of underlying infrastructure. In addition, we need to have complete visibility through users, devices, components and workloads across environments. Continuous threat detection is very important coupled with consistent user experience."

Vision for Security and Risk Management 2022

AkshayGarkel, Partner & Leader, Cyber, Grant Thornton Bharat states that supply chain security is going to be the way forward as it is crucial to understand the data flows, threats and profiling. "Organization's security is as strong as the weakest chain. And in majority of the cases people are the weakest link. Hence, people awareness and skill levels are crucial to avert any insider threat. Zero Trust is becoming popular among enterprises, however, we must note that it's not a product; it's a concept or a thought process to invoke a culture across the organization. Hence, organizations need to realign their processes to match global standards which calls for increased priority for budget and resource allocation towards risk prevention."

While the future is unclear and we don't have much clarity around how the pandemic will play out. Hence, the focus must be on the basics. One should assess the resilience of the infrastructure, make sure that devices are properly configured and there should be clarity around what we are trying to defend. We should give a solid platform so that the business can pivot in whichever direction they can, but with a secure foundation.

Jaspreet Singh, Partner and National Leader, Client & Markets (Trust and Transformation), Grant Thornton Bharat seconds that the entire decade of 2020 will be focused on digital trust. "In comparison to the scenario two years back when businesses were still deliberating on their move to cloud, organizations are already working on their strategy on cloud and cloud security. Organizations need to draw a clear roadmap from the current and future perspective. This push will ensure that cyber security will be the part of the discussion during the board meetings and all the business initiatives."

"Organizations need to draw a clear roadmap from the current and future perspective. This push will ensure that cyber security will be the part of the discussion during the board meetings and all the business initiatives."

Jaspreet Singh
Partner and National Leader, Client & Markets (Trust and Transformation), Grant Thornton Bharat

IoT will Drive Cyber Security over the Next Five Years: SonicWall

Debashish Mukherjee, Vice President, Regional Sales-APAC, SonicWall, shares that IoT will be a big trend over the next 2-5 years. With the advent of 5G and major adoption of IoT,the company is developing IoT-focused security solutions to remain relevant over the next five to ten years

Debashish Mukherjee

Vice President, Regional Sales-APAC, SonicWall

The ongoing pandemic has certainly increased the importance of security among the enterprises. What are the top trends you see in the cyber security market in India?

Organizations are primarily investing in remote mobility solutions. In addition, a lot of organizations are moving towards cloud or partially moving towards cloud. And, we are now seeing more activity towards the Internet of Things (IoT).

According to the recent 2022 SonicWall Cyber Threat Report, India witnessed an exponential 981 percent of ransomware attacks in 2021. Keeping that in mind, how would you assess the overall preparedness of the organizations in India?

In India, we do not have a strong compliance requirement from the government as of now. That is a reason many of the organizations are showing laxity and a lot of attacks are happening; probably many of the events are not getting reported. The MSMEs do not pay much attention to cyber-security. On the other hand, large enterprises are paying attention and are investing in cyber security to the extent, but not fully. Whatever traction we are seeing on cyber security is probably because they need to meet the global compliance requirements.

Cont'd on page.....16

What are the challenges that CISOs and security leaders are facing?

In India, many of the organizations still consider cyber security as an ad-hoc solution. However, cyber security is a journey; it is not about the firewall, email security or remote mobility. You need to create a plan once you understand the journey, but CISOs and CIOs are still not doing proper planning in this regard.

What is the level of adoption you are seeing for advanced cyber security solutions? Where do you see the enterprise focus moving towards?

Large enterprises are primarily looking to build an agile and elastic business model. Due to Covid, suddenly, the requirement of remote mobility solutions has gone up from probably 10 to 100 percent. Large enterprises are now evaluating what solution to adopt to be more elastic and have more visibility on their environment.

A new global climate and fast-moving market dynamics is accelerating the need for boundless cyber security, which proactively mitigates cyber-attacks across organizations' boundless exposure points, including a workforce of remote, mobile and cloud-enabled users.

The Boundless cyber security model theoretically has got three pillars. First is knowing the unknown. CISOs and CIOs should know what kind of attacks are happening in their network. Second, we must have visibility through a single pane of glass, which is called unified visibility and control. Whatever solution I have implemented, I should see how things are happening and collaborating. Third, we are talking about how we can make our business agile and at the same time how I can reduce the cost of security.

What are your thoughts about Zero Trust and if you can elaborate a little more on how you can relate it with SonicWall offerings and the solutions you have?

Zero Trust is needed at this point of time, primarily because we are all working remotely and eventually, I think this will be the standard business model in future as well. All our remote mobility solutions are offering Zero Trust. We have a lot of products which can meet Zero Trust now; it is build-in even in the boundless cyber security model.

> **"Large enterprises are primarily looking to build an agile and elastic business model. Due to Covid, suddenly, the requirement of remote mobility solutions has gone up from probably 10 to 100 percent. Large enterprises are now evaluating what solution to adopt to be more elastic and have more visibility on their environment."**

What are your suggestions to build a robust cyber security?

My first suggestion to the customers is to think from a layered approach. Do not go for a best-of-breed approach. Our idea is to protect your data and then you can start evaluating. Second, the customers need to see if the products are talking to each other or not. If your endpoint is finding out any threat and it is not talking to your centralized reporting tool and your firewall is not aware of the threat as well, then there is no point in the best-in-class product.

What are your top five focus areas over the next two to five years?

In the next two to five years, IoT will definitely be a big thing. Also, once the 5G comes, starting from refrigerator to CCTV, everything will be interconnected at home, following which you have to secure the network. That is why we are developing a lot of IoT-focused products so that we can stay relevant for the next five to ten years. We are upgrading and trying to focus on our solution centric approach.

Lending will Shape the Fintech Industry in a Big Way: Falcon

Chinmay Desai, Chief Business Officer, Falcon explains how the company is enabling financial organizations to co-create most innovative financial solutions and why lending is going to lead the Fintech industry going forward. He highlights his top-5 priorities as the company targets to achieve $1.5 in payment throughputs and $30 million revenues by 2023.

Chinmay Desai

Chief Business Officer, Falcon

How much do you agree with the fact that the pandemic has boosted the growth in the fintech industry, at least by five to six years?

I definitely agree with that. I think the pandemic has brought about logistical challenges. Corporations have also responded by adopting a very digital way of life. Fintech actually helps reduce the overall cash in the ecosystem. They brought the entire delivery of financial services to each and every household. Therefore, you see that most of the countries have shown more than double-digit, some even triple-digit growth in terms of intakes during both the pandemic and post-pandemic era.

How does Falcon add value to the digital journey of businesses and enhance their overall customer experience?

Falcon is a full-stack B2B embedded payments platform. We co-create the most innovative financial products. These are products of the future, and we enable India's and the world's most forward-thinking companies to embed financial services very easily in their system, literally in weeks. We are built on a modern technology platform - microservices architecture. We provide a modern user interface and a user experience for any ecosystem, be it digital or physical, to quickly embed financial services by leveraging capabilities so they do not have to go ahead and build all these financial services on their own.

What would you say is the USP of Falcon's API platform?

Falcon, being an API platform, connects to multiple issuers on

the supply side. I think companies can launch their Financial Suite ecosystem by only talking to Falcon. Our APIs are robust and flexible. Any company who would want to launch on their own, will have to speak to banks, will have to speak to networks, will have to speak to processors, then we'll have to speak to KYC companies. We are bringing everything as a bundled model in one ecosystem, in one platform, which is part of Falcon.

Please talk about your recent business achievements in terms of business expansion, revenue growth and customer acquisition.

On the growth side, you are seeing extraordinarily strong indicators. It is both on the demand side as well as on the supply side. First, let me talk about the supply side. So, banks, financial institutions, and NBFCs across the ecosystem, not just in India but across APAC, Middle East, and Africa, have reached out to us to use our platform for last-mile delivery for their customers and their fintechs. On the demand side, we have seen incredible demand across multiple sectors for the Falcon Financial Suite across India and the global markets. Since Falcon emerged from its stealth mode last quarter, we have seen a ten times growth in payment numbers. I can confidently say that we are on track to achieve $1.5 in payment throughputs and $30 million revenues by 2023.

Please talk about your top five focus areas over the next 12 to 18 months.

The first focus area would be to build an A-plus team. Second is to create a solution stack. In addition, we are looking for strategic alliances as we realize that we cannot build everything on our own. Therefore, we are building our alliance system to make sure that all our product partners are also coming into the product ecosystem to build that solution stack. The fourth area is to get our own licenses. And then the fifth focus is the merger of the previous four priorities, which is revenue and market share.

What trends do you think would shape the fintech industry in the next couple of years?

There is an 87 percent adoption rate for fintechs in India, which is the highest. There are some pockets in India, which are using financial technology more than WhatsApp.

In addition, the digital lending industry is going to touch $350 billion. That means there are a lot of NBFCs, banks and financial institutions like Falcon, which are going to come and lend to make sure that every consumer can get what they want. There are going to be credit scoring mechanisms. So, lending is going to shape the fintech industry in a big way. Over 500 million users are expected to get access to financial services, either through smartphones or through traditional channels.

Another important trend that I see is partnerships of fintechs with traditional players in banking, insurance, retail, and healthcare. This will bring the entire ecosystem into the gamut of the financial ecosystem.

Further, the regulator is showing great interest in fintechs. Since RBI has now created a fintech department, more autonomy for fintechs is on the anvil. That will remove friction and will further lower costs.

Then there are technologies like artificial intelligence and machine learning, which will help sharpen the financial offerings. So, this is how fintechs are going to grow.

"The first focus area would be to build an A-plus team. Second is to create a solution stack. In addition, we are looking for strategic alliances as we realize that we cannot build everything on our own. Therefore, we are building our alliance system to make sure that all our product partners are also coming into the product ecosystem to build that solution stack."

Four Principles are Critical for Strengthening Security Postures

While elaborating on tips to strike a balance between adequate security, access, and employee experience, Mohit Gupta, Group CISO, Motherson Group, shares four principles which are critical for strengthening security postures of the organizations

Mohit Gupta
Group CISO, Motherson Group

What has been your strategy to secure systems in a distributed network?

We went for a refreshed risk assessment covering all endpoint types, all identity types, irrespective of whether it is a local user, a local admin, or a privileged account. But then, to be able to address all of it, we obviously had to pick some of the solutions. So, it could be in the form of EDR, MFA, PAM advancement and SOC to gain speed especially around those sole use cases. We again went ahead and refreshed our overall incident response plan to even cover more aggressive response mechanisms. The special focus has been around this privilege to support end users as well.

Do you also have some of your own technologies?

Yes, we have nearly 20 odd different custom applications, which are not only used for our business applications, but for our security needs as well. Irrespective of what we do, especially when it comes to integration, there is a lot of middleware that we had to create to be able to have this and to be able to gain the speed of how we respond to adverse situations.

How do you enable a balance between adequate security, access, and employee experience?

I would like to talk about two important things- foundational areas and employee convenience. User convenience should be one of the criteria. The way we are monitoring our security control implementation is a concern. The second foundation that I must highlight is protecting the employee identity. Also, when you strike this balance of user convenience over security, picking up technology is one aspect of it. But how effectively, efficiently, and smartly we are implementing those technologies is very important.

What should be the updates in the incident response approach for an organization to make itself resilient enough to identify, prevent, and recover from any disruptions that may arise from new threats, vectors, and attack techniques?

Data security and privacy regulations are evolving across the world in many geographies. You rightly use the word resilience that can only be done when we make sure that we incorporate all these aspects into the plan itself. So, we need to plan very deeply and very effectively. If at all, we don't know, we should involve experts, and make sure that we incorporate each of such elements and prepare ourselves for the worst.

Do you think emerging technologies can act as an enabler to cybersecurity or are they just an area of concern for the CISOs? And how can organizations utilize such technologies to strengthen their cybersecurity posture and gain a competitive advantage?

Well, no one would deny that these emerging technologies are certainly important. I always focus on four core principles. The very first is security by default which is a cultural change to incorporate security in the solution planning itself. The second is defense in depth. The third principle I always admire is the solution, and any of the technology that we adapt should be scalable and agile. And the last important core principle is resilience by design. Again, not just to focus upon how to get back to business after something goes wrong, but important is how do we position the business to elevate the brand equity if something goes wrong, and gain and sustain the stakeholder's confidence. I guess that is where the answer towards cyber resiliency lies.

What are your suggestions on the cyber resilience strategy and tips to help CISOs that will help recover from incidents quickly with minimum possible damage?

Let me first talk about one of the very important aspects, which is having complete visibility to your CMD. Not many enterprises do maintain CMDB to an extent that contains the utilities, and each of the software and assets that are there into their environment. There are a lot of blind spots. It is very important to have your response plans ready covering all possible scenarios that you could think of. Make sure that we remain agile and alert to the situation because no matter how much preparation that you do, we must readjust our approach when we are in the middle.

“I would like to talk about two important things- foundational areas and employee convenience. User convenience should be one of the criteria. The way we are monitoring our security control implementation is a concern. The second foundation that I must highlight is protecting the employee identity.”

Spice Money is Sponsoring Education for Merchants' Girl Child and Financial Literacy for Wives

Varundeep Kaur, CIO, Spice Money, believes that organizations are becoming more inclusive of women, however fintechs are still lagging. She also mentions that talent is not divided between men and women and if there are no areas of opportunity, we should go ahead and create one

Varundeep Kaur, CIO, Spice Money

We want to hear from you about your journey and the ups and downs so far.

I started my journey close to two decades back with my higher studies in engineering. Then I joined Spice Telecommunication at that point in time that opened the entire new space of technology for me. Then I moved to Spice Digital MTS, and now I am with Spice Communications, taking care of fintech as a CIO. So, it has been a quite enriching and challenging journey so far. And I would say I am blessed to get lots of opportunities where I got to play different roles as a team member, and then leading the ladder and stepping up the ladders to reach this leadership position. So, it has been really nice.

Women are playing in driving this innovation?

As per the reports, it is mentioned that women empowerment and innovation are there. Their inclusion into the space moved to require digital literacy, financial literacy, and obviously technology. And with combination of this with access to all this information to urban women largely and to some extent to the rural woman. So, we see a lot of people coming in. Since women are more observant of the problems that somebody is facing, they are coming up with a lot of innovative options like financial illiteracy, or how they can help other people get into financial inclusion, which through government initiatives directly is not possible. If I take a specific example of Spice Money, we are pushing for a lot of women Adhikaris. We call our merchants Adhikaris. And we see an upsurge, and during the pandemic time in the woman Adhikaris, and we see that they have gone out of the way and come up with a lot of innovative ideas. So, we will see women taking up more leadership positions and a greater role where they can be more inclusive as well as they can provide us better ideas on how to bring this fintech situation better.

If you can elaborate a little more on what they do and how you identify these Adhikaris and how is the engagement?

There are two main large problems that we are looking at. If you go by statistics, you will find close to like six lakh villages are there in India and close to 1.25 lakh bank branches and ATMs. The appoint merchants who become assistants or provide the last mile assistance to the customers, like if somebody has got money in their bank account, they can simply go to the merchant counter, give their Aadhaar number and biometric thumbprint and they can withdraw and deposit the cash, they can check their balance, they can check statements, and they can also do remittances well. And then there are other services also like paying bills, doing recharges, booking hotels, train, flight and bus tickets as well.

When it comes to managing their own funds, they still are so much dependent on their male counterparts. What is Spice Money doing to enable women financially?

As a CSR initiative from our side, we have told our merchants that we will be sponsoring their girl child's education for a year and we will also empower and impart

the financial literacy or financial education to their wives, so that they can participate along with their male counterparts who are into the business so that they can learn. And then we are also thinking of how we can introduce more ways and means where women become more aware, because we have understood that they are very good at relationships and if there is a customer problem, they will go out of the way in order to get a solution. So, with this, there are a lot of financial products, which are coming up in Spice Money and a lot of fintechs are also coming up which are boosting financial literacy and education for women. In Orissa, we have already done this project called Shakti where women VCs are there and we have partnered with banks in order to provide these services. We have set up a platform which is called Cha Cha, where we meet and interact with the woman Adhikaris to know how they are using that information, whether they are getting something to earn or not, if yes then the next step is educating them in how they can multiply their own money and how they can generate more money out of the money that they have.

What are the challenges you see which are keeping women representation at the lower end?

One if you go by ILO, this Gallup survey of 2016, so, there is still a kind of a mentality that exists where women should not participate in paid jobs. There were around 20 percent of men who felt like this and around 14 percent of women who felt like this. So, first there is gender bias where certain people think that women are more apt for home roles rather than taking an outside role. Further, there is a 25 percent increase in terms of participation between men and women. And the larger challenges have been there where the roles are stereotyped based on men and women. Also, the proximity to job location and lack of affordable care have also been the issues. There is also a pay partiality. So that is also one of the reasons and areas where men will feel that I am getting this much package and you are earning this much package, so take care of home and I will manage the finances.

What is the level of engagement you see from women in the fintech ecosystem and how does the FinTech ecosystem help aspiring women to take those leadership roles?

I believe now organizations are becoming more inclusive. However, I see that in the organizations which are getting founded for fintechs, there is still very less participation. You will find at global level there are only seven percent of women-founded organizations that exist. So the participation of women has to actually improve and we have to add on to it.

Talking about Nari Shakti and the initiative of Spice Money to get them connected with the VCs, how are you building the grounds to enable more women to take up entrepreneurship and what women need to do to inculcate an entrepreneurial spirit?

First women must stop thinking of themselves less. So, one is that they must be aware, they should invest effort in networking and mentorship. And what we have seen is that we must encourage the women participation at VCs and the leadership roles also. And what I believe is that in order to encourage that, organizations should also start with the entrepreneurship kind of efforts or initiatives where they give a woman an opportunity to lead certain initiatives. Our organization, Spice Money, has also started this kind of initiative where we are now encouraging ownership, where few women leaders will also mentor some of the ideas. In addition, what I believe is if there is a woman in the investing side of it, be it VC or angel investing, there is more likelihood that they will invest into woman-oriented or woman-led organizations.

Please talk about your interest areas and hobbies outside your professional life and family responsibilities.

I am an avid reader. So, I go through a lot of books and try to find out where I can fill in the gaps which I, as of now, have not been able to solve. On the technology side there are a lot of new technologies that are coming up like blockchain and metaverse. Apart from that I like connecting with the people; I try to know more about them and how we can create a better organization or platform for them and even on the other side of it, how we can create better humans with more inclusive teams.

What is the message you want to convey to the aspiring women leaders and women in technology?

I would say women should stop thinking less of them, they should just go about whatever they feel, and it is not that only women will feel resistance or pushback, it is true with the men as well. You should not give up. It is that you may not taste success in the first go. However, if you keep on trying to set the example for others you never know for somebody you are setting that inspiration or that kind of example where other people will also follow you. So don't give up. Take the next step. Get into more networking and mentorship, ask for help wherever it is required rather than stopping and making it a full stop. Talent is not divided between men and women. If there are no areas of opportunity, we should go ahead and create one.

Our Key Focus is to Innovate Supply Chain: Otipy

Otipy is focusing on innovating the supply chain as it is the key to fast movement of the goods from farm to fork. Vikas Bothra, VP Finance, Otipy, mentioned their expansion plan to other cities including Mumbai in the next month and to other countries in the next quarter.

Vikas Bothra, VP Finance, Otipy

How's Otipy positioning itself to add value to the agriculture industry?

We are primarily into the agritech supply chain. When we started in 2016, primarily we were doing B2B. Currently, we operate under the brand name of Otipy from March 2020. And over a period of the last three years, we have seen a lot of unforeseen circumstances. Our primary focus is to deliver fresh produce in the consumers' hands within a period of 12 to 15 hours, reducing our vestiges to supply pressure.

Agriculture industry has been operating on a five-layer business model including farmers, farm agents, wholesalers, retailers and consumers. We get this produce directly from the farm gates reducing wastages because our resources are low. We incur only five percent wastage losses, and pass on the benefit to the consumers as well as to the farmers. So, what farmers get is the right price as well as they get direct feedback from us in terms of what quality to grow and which produce to grow.

The recent study at Harvard Business found that many finance teams struggle with accurately preparing, reconciling and accessing the high volume of information or integrating the recent or the real time data into analytics. How do you think the finance team of these startups or SMEs with a strong digital vision should align the financial goals with the business?

The startups at the initial phase are very unstructured. At the same time, they are very agile and can adapt to new situations very quickly. Similar was the case with us back in March 2020. I remember, although we shut all our operations from head office immediately, for about one month, we were operational with full force at our warehouse. And during this time, to my surprise, we started using cloud technology on our day-to-

day operations that made people switch to the technology where people can work even remotely as well. So, there's a larger need for technology now. And with the technology tsunami coming in, and in the last two years, it has taught people to adopt it even in multiple fields, not limited to the businesses, but also how you manage it.

CFOs need to work closely with the CEO, to sell the IPO story to the investors. We wish to understand your experience, your approach to the IPO process including the pain, the joys and the lessons you've learned from the process.

I've been into this space for the last 12 years and have seen a lot of fundraisings. At Otipy, what I keep saying over regularly is that whatever fund that we've raised, we should think in a way that we got to return more than what we have raised. So, at startup, I suggest to raise as minimum capital as possible and become self-sustainable. Raise capital very wisely and think it from our perspective that you got to return these monies and help build this business as sustainable and profitable.

For businesses to go for an IPO, the first step is to have a good banker and counsel. In addition, the business needs to have a very strong team that could work dedicatedly on the IPOs. And above all we must look at the financial readiness on the basis of financial statements and results; then only go for IPO.

How difficult or how challenging is it to build a good talent pool especially within finance?

In the last two years, it's been quite a talking point about the less availability of the candidates across functions. Obviously, technology has been a talking point. But slowly, this disruption has also been coming to the other functions as well, like finance. The approach that we have taken is you have to have the right balance of the interns and the experienced personnel in a balanced way. Because with the interns you get, there are a good number of candidates, and these people are very enthusiastic to have a balanced approach now.

Can you just share your roadmap for the funding in the agritech and the farm to home delivery startups?

Investors are looking at this business very positively, provided you are able to grow it sustainably and you are able to deal with the wastages. Last year, we closed our Series A round of funding, and this year again we closed our series B round. Along with the existing mission, it will be around $32 million. Now, we are planning for the next round of funding.

> **“Investors are looking at this business very positively, provided you are able to grow it sustainably and you are able to deal with the wastages. Last year, we closed our Series A round of funding, and this year again we closed our series B round.”**

How are you leveraging the technology to drive a farm-to-home delivery model to reduce food wastage?

Technology helps us in reducing our wastages and helping us ship these products in a fastest ever supply chain period of like 12 to 15 hours. When placing an order, the harvesting happens apparently, not technically, even as we speak today, we don't have any produce at our warehouse; these produce are getting harvested at the farm gate. At night these products will reach our house and within three to four hours of the timeframe, our supply chain will process them and will deliver them to the community leader early in the morning.

What are your key focus areas for the next two years?

Technology is at our heart. So, firstly we will continue to invest in technology and innovate our supply chain as well. Because supply chain is key to fast movement of these goods from farm to fork. Then we will continue to add categories. We'll be pouring into multiple cities in the coming years. We are already opening in Mumbai probably next month. And last but not the least, obviously to make this business profitable.

Any plans to go overseas?

So, with the innovations that we have done in the supply chain, we are getting a lot of interest from overseas regions including Africa and Southeast Asia, to start operations there. So probably in the coming quarters we will decide and move accordingly.

We are moving towards an Assisted Digital Model: Shivalik Bank

Ankit Khare
CTO,
Shivalik Small Finance Bank

Ankit Khare, CTO, Shivalik Small Finance Bank, shares that banks are now looking at offering their banking services over unconventional or non-traditional channels such as WhatsApp. The bank is targeting to move to a more assisted digital model and reimagine retail banking through a digital lens with partnerships with fintechs and neo-banks

Over the last two years the BFSI sector has been facing continuous disruptions from the pandemic as well as the technology, so what are the top three challenges you see off late in the banking business?

From a business standpoint, I think collection and recovery continues to remain a problem for banks, so is maintaining the NPA numbers. Since the customers now have kind of got used to doorstep banking services or services over online channels, it has become important for everybody around to get on to that digital bandwagon quickly and start offering their services accordingly. This might not be a challenge for large players, but I definitely pinch the smaller ones. From an employee standpoint I think maintaining the employee productivity while ensuring the compliance to regulatory and cyber security norms is another challenge. Also, getting them to work remotely remains a concern.

How do you see fintechs, as a competition or as a collaborator to enhance your processes and become an agile organization?

So, what makes fintechs standout is not just the product and services that they offer, it is the kind of experience that they're offering to their customers that is very different from what the customers are used to having from the banks. Now, this is something that I'm sure banks are finding it very difficult to catch up with since that has never been their strong point. And that is pushing them to revisit their business and tech strategies. Having said that, I think the product offering that the fintechs are bringing to the table are only as strong and mature as the banking system that has been powering them. So essentially, what I see is an opportunity to collaborate, co-build and offer the best of both worlds to the customers while strengthening each other simultaneously.

Why do you think that collaboration with fintech or insurtech companies is crucial for banks in India?

Growth in the fintech sector in India has been rapid and we have become the third largest fintech ecosystem. Areas such as digital lending, insurance and neo banking have seen a lot of small and large fintech players proving their mettle. So, banks need to catch up. They may attempt to match the experience they are offering to the customer. What is more practical is to collaborate and leverage the popularity

that these fintechs have in the outreach that they have built to gain access to customer segments and regions beyond banks' physical presence to offer bespoke and curated products and services to the customer. Also explore the possibilities to cross-sell as well. I think that is going to be a better proposition for the banks to work upon.

So, according to you, what are the trends you see in the technology adoption in the BFSI sector?

Banks are now looking at offering their banking services over unconventional or non-traditional channels such as WhatsApp. Banks are adopting a lot of tools to automate the customer interactions, sending across reminders or payment links. RBI has helped in by allowing video KYC as a medium to complete a full KYC, which was not the case earlier. With that we did touch upon possibilities of integration, or partnerships with fintechs and insurtechs. Now, that would only happen if you had a very strong integration on an API capability. And lastly, coming down to the infra part, I think the cloud-based offerings have picked up off late and they've become an important part of technology strategies.

As you rightly said that automation helps accomplish mundane tasks without much human intervention, reducing cost and increasing efficiency. So, how aggressive are the banks in automating their processes?

Banks have definitely picked up pace in their automation journey with the push coming primarily from the digital transformation and the need to offer better customer experience. So, while improving efficiency and reducing costs definitely is the underlying thought. The focus has been on cutting down the resource utilization in the routine and the back-office jobs and, realigning that workforce into driving innovation especially in the digital banking space. APIs necessitates any manual intervention to be done away with to support STP if banks actually wish to go digital in the true sense.

What are your recent initiatives around digital transformation?

We are working towards our vision to reimagine retail banking through a digital lens. A lot of our focus of late has been to standardize our banking service, allowing us to partner with fintechs and Neo banks and solve various customer cohorts. We have built capabilities to end-to-end service our customers including onboarding, opening accounts, deposits, managing a lifecycle, loan, lifecycle payments cards, to name a few. And we've already been working with some major fintechs and API aggregators in the country in the space of Neo banking, gold loans, agri-loans, microfinance, deposits, etc. And this is not just for an external use case, even internally also we are using the API stack that we've built to onboard and service our customers across various online channels that we have including internet banking, mobile banking, IVR, SMS, web agent, or tap banking.

Small finance banks often face challenges on certain restrictions and trust deficits against their bigger nationalized counterparts. How is Shivalik Small Small Finance Bank benefiting with focus on digital transformation?

We have been working towards limiting our customers' need to actually physically come down to any of our branches to do business with us. We are trying to move to a more assisted digital model, rather than just a physical interaction. The strategic partnerships that we have done with fintech players and Neo banks which has helped us leverage their presence and brand building that they've already done to offer our services rather than putting us out as an independent player. So, we kind of piggyback on the presence that they've built, to reach out to the customers and offer our product and services to them, and allow them to exchange or do business with us without actually the need to come down to any of our branches.

What is your outlook for the BFSI industry for the next two to three years and what are the key technologies that you would focus upon in 2022 and beyond?

The BFSI space continues to evolve and reshape the way we rank fintechs. Neo banks are definitely going to lead with a larger market share from what they have at the moment. In this segment the collaboration with banks definitely is going to continue. Both entities have very strong areas that they continue to develop and then collaborate and offer better to the end customers. For the banks, the focus is going to be on developing the non-traditional alternate channels. I think banking is going to move more towards a necessary digital model. You'll see less resources are being deployed at physical branches and the banks will keep investing into having more and more kiosks and automated setups that are going to be around in these branches. Again, open banking and SaaS continues to take the lead. I would say we are looking at a very disruptive outlook in terms of banking in India and obviously globally as well.

We Fully Operate from DR Site for a Week Every Quarter: BSE

Shivkumar Pandey, Group CISO, BSE highlights that with the increased attack surface in addition to the upsurge of zera-day and malware attacks, it is crucial to streamline DR strategy. As a best practice, BSE fully operates from its DR site for at least a week every quarter to streamline things and fill the gaps proactively

Shivkumar Pandey
Group CISO, BSE

How has the ongoing pandemic changed the dimensions of digital transformation as compared to the pre-pandemic times?

The adoption of digital transformation, digital technology and cloud has taken a quantum leap and has fast-forwarded the process by several years. The funding of the digital initiatives has exponentially increased in the last couple of years. Now, it is especially important to give cybersecurity training to all the employees. In addition, implied productivity software are also coming up where the organizations can monitor what their employees are working on.

What are the key critical challenges for a CISO today especially after the impact of Covid-19 has changed the business priority of most of the organizations?

The work from home concept or the work from anywhere concept is a big challenge for us. The zero-day and malware attacks were already there and now the attack surface has also increased.So, new concepts are coming up. In the current circumstances, zero-trust cybersecurity framework and adoption of those policies will help strengthen

security.The cloud adoption, hybrid cloud-based services and data localization are other big challenges for organizations.

What are the challenges you face in your data protection efforts? And if you can talk about your data protection strategy?

We have stringent data security and data privacy policies which are implemented across the organization. It depends upon the menu, regulatory, and the standard framework.Maintaining and securing the data while we collect from the customer is a fruitful area of focus for us. We manage complete data management cycle of the given data. We do the data flow analysis and data lifecycle management from the beginning. In addition, data leakage prevention, data classification, data encryption, and data maskingarefew of the technologies we have implemented to safeguard our data and data privacy.

Please talk about your next-gen SOC.

We have implemented our next-gen SOC five years back only. There are more than 14 niche technologies over there. So, deployment technologies like data analytic forensic tools and UVA are the kinds of our Access Management System. In this next-gen SOC, we have a subscription from domestic as well as the international threat intelligence feed, and the USP of this next-gen Cyber Security Operations Center is all about cognitive and machine learning technology, which can provide deeper insight by ingesting and understanding the exchange of data sources including human-generated data like blocks.

“We have implemented our next-gen SOC five years back only. There are more than 14 niche technologies over there. So, deployment technologies like data analytic forensic tools and UVA are the kinds of our Access Management System. In this next-gen SOC, we have a subscription from domestic as well as the international threat intelligence feed.”

What are the best practices to ensure backup recovery and replication for all your applications and data?

We have real time data backup and replication. We are even using synchronous and replication approach to our DR and PR site. As a best practice, we fully operate from our DR site for at least a week every quarter. Further, it is a dish-to-dish backup of all the details, which is again on the encrypted format; no lateral movement is there. In addition, the BCP and DR Policy is practicedby everyone in our organization. In fact, we fully operate from our DR site on the weekends. This enables us to streamline things and fill the gaps proactively.

We are technology-driven companies. We are providing our platform to offer trading services for you.The per day trade transaction are over 700 million orders and we are operating that in six micro-seconds. So, you can understandwhat kind of value we are carrying in it.

What will be your key security focus areas for the next two years?

The first is the zero-day attack which is a new malware attack. New ransomware attacks are anyways there. In addition, spear phishing attacks are increasing a lot because human being is the weakest link. Hence, we need to provide cybersecurity training and awareness to all the stakeholders and it is not only for your employees, but you also need to provide cybersecurity training and awarenessin your complete ecosystems. Since, everything is shifting to the cloud now, there will be lot of regulations coming on the cloud front as well.

BenQ Dominates Projector Market with 30% Share in Q1'22

The Futuresource Consulting report has named BenQ as the #1 brand in the overall projector category. The company registered a 30 percent market share in both B2C and B2B projector segments in Q1 2022, as per the recent report.

The demand for large screens to watch movies and other entertainment at home is driving the market for high-definition projectors. Covid-19 has also been a catalyst contributing to market growth in the home video segment.

As per the report, sales volume in the 4K UHD resolution segment increased by 34 percent YoY in Q1 2022, and BenQ was the industry leader with a market share of 53 percent. Moreover, in terms of sales volume, the portable projectors for the home segment grew by 82 percent YoY in Q1 2022, with BenQ leading the market with a 50 percent market share. Another form factor that has seen stupendous growth is the 4K Laser TV in which BenQ has a formidable 51 percent market share.

Q1 2022 also saw the reopening of educational institutes and corporate offices. This led to the increase in demand for B2B projectors. In this sub-category, the WXGA segment grew the most in volume by 108 percent YoY and BenQ is the market leader with a 50 percent share in Q1 2022. BenQ is also the number one brand in the Full HD data projectors with a 27 percent market share.

Analyzing the market segment basis light source, there is a clear trend visible in terms of customer preference. While the conventional lamp segment experienced a growth of only 32 percent, the Laser Light Source segment grew by a whopping 150 percent in terms of sales volume in Q1 2022 compared to Q1 2021. Another significant shift has been towards the preference for the LED Light Source segment which increased by 54 percent in terms of sales volume in Q1 2022 indicating that the market is moving towards solid-state light sources instead of traditional lamp sources.

Rajeev Singh
Managing Director, BenQ India

Rajeev Singh, Managing Director, BenQ India, said, "We are delighted and honored to be acknowledged as the No. 1 brand in projectors by Futuresource Consulting. With the reopening of educational institutes and offices and the continued booming demand from the Home segment, the projector category has overall seen a growth of 38 percent and BenQ has experienced a growth of 62 percent as compared to Q1 2021. Customer preference is moving towards high-end projectors wherein 4K resolution, solid-state light sources and accurate colors are the key drivers."

Brother Names Alok Nigam as Managing Director for India

Alok Nigam
Managing Director
Brother International India

Brother International India has appointed Alok Nigam as the Managing Director for India business, effective from April 1, 2022. Nigam succeeds Shigeru Morita, who led the company successfully for five years.

Nigam is the first Indian MD of Brother India since the company's inception in 2007. He has almost 25 years of expertise, including 10 years with Brother India.

Commenting on the appointment, Morita said, "Brother has achieved many important milestones over the years, and I am enthusiastic about this new change. As a well-experienced and highly effective leader, Alok brings a wealth of knowledge and expertise to this position. I wish him all the best for the future."

Speaking on his new role, Nigam said, "It is a real privilege to get this opportunity to lead business In India. India is a key market for Brother group with tremendous opportunities. I am looking forward to create value for all our stakeholders along with a steady growth in our market share."

Nigam has a Masters in International Business from the Indian Institute of Foreign Trade in New Delhi, as well as a Bachelor's degree in Mechanical Engineering.

Channel Point

Security Breach is the Biggest Factor to Halt Organizational Growth, Profitability

Strengthening the fact that digital trust is the most important currency in the current scenario, the cyber security experts are agreeing that security breach continues as the biggest factor to halt organizational growth and profitability. This is further boosted with the ongoing Covid-19 pandemic that the world is facing over the last two years. COVID-19 and consolidations have reshaped the cybersecurity market. Channel partners and customers must keep up with the market and best practices, including insurance policies. An understanding of the cybersecurity market can help.

Businesses have ever-growing amounts of data to manage, and it is now exposed between all kinds of remote applications and locations as a result of how we now work. Existing technologies have required adding more and more products to a noisy and complicated security stack. The average company has 76 security products, and effectively managing these is impossible.

Cybersecurity companies are working towards the simplification of security by taking it into the cloud. By using one policy to rule them all, and delivering things like Zero Trust over SASE architectures, suddenly cybersecurity provision can scale to the size of the business, and how modern employees actually work. CISOs need to discuss the business impact in terms of revenue loss, reputation loss, and regulatory fines that follow after the security breach. Above all, we need to assess the competitive advantage which comes as we showcase resilient-by-design architecture to the potential customers. Digital trust is crucial in the current scenario.

Zero Trust is becoming popular among enterprises, however, we must note that it's not a product; it's a concept or a thought process to invoke a culture across the organization. Hence, organizations need to realign their processes to match global standards which calls for increased priority for budget and resource allocation towards risk prevention. Moreover, it's important for board level executives, to understand that it's impossible to protect everything, and learn to prioritise the most critical information, data and systems to protect. Businesses need to clearly understand compliance, the regulatory environment under which the business operates, what's legally required when breached and what are the appropriate controls around data security and management.

KALPANA SINGHAL, Editor
(E-mail: kalpana@techplusmedia.co.in)

TECHPLUS MEDIA

EDITOR: KALPANA SINGHAL
CONTENT HEAD: Amit Singh
ASSISTANT EDITOR: Rajneesh De
CORRESPONDENT: Aaratrika Talukdar
CORRESPONDENT: Atreyee Chakraborty

INTEGRATED MARKETING COMMUNICATION:
Aakash Vahal
Saugata Mukherjee, Mamta Dhiman,
Nishit Saxena

ASSOCIATE ANALYST
Shaithra S

SALES:
Harpreet Singh | Pratap Jana

PRODUCTION HEAD:
Aji Kumar

WEBSITE:
Sheetal Varshney/Ramesh Kr

PROMOTION:
Vikas Yadav /Amit Pandey

CIRCULATION:
Pratap

FINANCE:
Inder Pal

HEAD OFFICE:
370A, Sant Nagar, East of Kailash, New Delhi
Tel: 41625763, 26237405, 41620042
Email - kalpana@techplusmedia.co.in

MARKETING OFFICE:
10 UF, West Wing, Raheja Tower,
MG Road, Shanthala Nagar, Ashok Nagar,
Bengaluru, Karnataka-560001

Delhi: 9711841991 | **Mumbai:** 9711841992
Kolkata / Guwahati: 9331072026
Bangalore: 9354347953

OWNED, PRINTED & PUBLISHED BY ANUJ SINGHAL Printed at Modest Graphics Pvt. Ltd., C 52-53, DDA Shed, Okhla Industrial Area, Phase - I, New Delhi-20, Place of Publication: 370A, 2nd Floor, Sant Nagar, East of Kailash, New Delhi-110065, Editor- Anuj Singhal

#1 Backup for Service Providers

Exceed Customers Service level agreements (SLAs) while increasing margins & revenue

VEEAM | CSP PARTNER PROGRAM

Postal Registration No. - **DL(S) 01/3377/2019-21 Posting Date - 13-14, 27-28**
Registered with Registrar of Newspapers of India under RNI No. **DELENG/2010/32787**

OWNED, PRINTED & PUBLISHED BY ANUJ SINGHAL, Place of Publication: 370A, 2nd Floor, Sant Nagar, East of Kailash, New Delhi-110065, EDITOR: Anuj Singhal