Manish Chandegara,
Ex-IT Head and CISO Insulator Business Grasim Industries Limited (Aditya Birla Group).
Briefs about increasing cyber-attacks and data security.

Interview of Manish Chandegara,
Ex-IT Head and CISO Insulator Business
Grasim Industries Limited (Aditya Birla Group)

Do briefly tell us about your journey so far.

Highly skilled professional with more than 20 years of experience in driving vision and road mapping across various assignments and in architecting business solutions using ground-up development

Proven competency in **IT Infrastructure Operations, Project Management, Process Enhancement and ERP Implementation**

Received Award from Microsoft COO for successful implementation of AZURE Microsoft Cloud in Maahi Milk Producer Company Ltd., Rajkot

Skilled in **IT Infrastructure Management** by Layer-wise management of computing hardware, virtualisation, middleware, networking & storage

Proven success in **strategic planning & building IT solutions** involving selection of appropriate technology, finalizing Service Level Agreements for timely & successful completion/delivery of the projects

Managed:

- Audit of ISO 9001 2000, OHSAS, and BS7799 (Int. auditor for Adani Port IT Dept.)
- ITGC Audit for Adani Group, Magna Automotive, and Maahi Milk Producer Company Limited

Hands-on experience in designing, deploying, administration, maintaining & supporting **Windows, Citrix, Cloud, (MS Azure & VMware Administration**

Proven record of setting up & supporting all areas of IT Infrastructure with expertise in **System & VMware Admin., Networking & Security**

Successfully **analyzed information system needs**, evaluated end-user requirements, **designed custom solutions and troubleshot complex information systems**

Led a team of resources for operations & management of entire (OCC) Operation Control System on 24X7 basis.

Managed implementation & initiated the operation of OCC with standard & guideline of **France and USA OCC** in a short time period.

Headed operation of OCC, India and provided remote support for 250+ production server (Including SAP ERP) and mainframe systems including 2 major data centres in France and USA

Defined/ implemented IT policy & standard process as well as budget planning & expense conformance while guide the team for day-to-day service support to 84 plants in world (remote support)

Spearheaded implementation of IT infrastructure of OCC India centre along with planning for execution of infrastructure projects for India based plants

Briefly share your contribution in improving an organisation's efficiency & data security.

Implemented PAM, MFA, Intune, crowd strike, XDR & EDR for data security &

Concentrating on securing the walls around data seems to be the focus in many organizations, with almost 90% of security budgets spent on firewall technology. However, there are hundreds of potential ways to circumvent a firewall; including through customers, suppliers and employees. All of these people have the ability to bypass

Manish Chandegara
Ex-IT Head and CISO Insulator Business
Grasim Industries Limited (Aditya Birla Group).

exterior cyber-security and misuse sensitive data. For this reason, you need to ensure that your security efforts are focused around the data itself, not just the perimeter.

It's easy to visualize threats originating from outside your organization, as these are often represented in news and television as the biggest and most costly ones. However, the reality is that it's your insiders that can potentially hurt you the most. Due to their nature, insider attacks can be difficult to detect and prevent. It can be as simple as an employee clicking on an email attachment they believe to have come from a trusted source and releasing a ransomware worm. These kinds of threats are the most prevalent across the world and the most costly. Make sure that all data is stored in

an encrypted format and remains encrypted during migrations.

If you think installing an antivirus on every computer or device will protect your company from attacks, think again. As recent data breaches have shown, hiring a professional organization to conduct a security audit will always reveal weaknesses you were not expecting. I encourage you to take a walk around your office and look at your employees' desks. I guarantee, if you look hard enough, you will spot a password written down on a sticky note.

Inspite of the latest technology and software being used why are the cyber-attacks increasing? How can it be secured?

The adoption of cybersecurity solutions is expected to grow with

the increasing penetration of internet among developing and developed countries. Also, the expanding wireless network for mobile devices has increased data vulnerability making cybersecurity an integral part of every single organization across the world

Keep zero trust architecture in place, never trust any inbound connection request,

Keep updated all security tools, always try to keep critical server behind firewall

Share one of the most interesting assignments that you handled?

Implemented MS team during Covid 19 lockdown where in no any employee was coming office entire implementation was done online over VPN & remote access.