**MAHESH GARG,** *CEO at FLYONIT*

Mahesh has over 13 years experience in planning and developing IT infrastructure for various businesses and organisations, using Azure and other cloud platforms. He is a Microsoft Certified Azure Solutions Architect Expert, Azure Administrator Associate, and DevOps Engineer, with excellent knowledge of Microsoft 365 and Microsoft suite products. His core competencies include designing, installing, configuring, and maintaining enterprise-level cloud solutions, aligned with business needs and security standards. He also provides technical guidance, assessment, and consultation for active directory, cloud technologies, business continuity, disaster recovery, and cloud-native applications.

## TIP 1. EVALUATE YOUR SECURITY POSTURE

The first thing to do is to conduct a thorough security risk assessment in the company to identify potential vulnerabilities. Understanding the impact of various threats on your operations, whether they stem from system failures, natural disasters, or malicious activities becomes very crucial.

## TIP 2. EDUCATE YOUR WORKFORCE

Provide comprehensive cybersecurity training to all employees, keeping them informed about common scams, phishing techniques, and evolving threats. Also, because cybersecurity threats are constantly evolving, make sure, your training curriculum is relevant and updated frequently.

## TIP 3. USE MULTIPLE LAYERS OF PROTECTION

Implement a password policy that requires strong passwords and monitor your employee accounts for breach intel through technologies. Implementing mandatory multi-factor authentication and encryption protocols is the best way to safeguard your network and endpoints from attacks.

## TIP 4. KEEP SOFTWARE UPDATED

Keeping your software up to date is paramount for safeguarding your security. Failure to patch vulnerabilities exposes us to various cyber threats that can compromise our systems and data. Cybercriminals exploit these vulnerabilities, employing diverse tactics to infiltrate computers and access sensitive information. MSP (or Managed Service Providers) automate this process of software updates, ensuring timely protection against emerging threats. Additionally, it's also essential to extend this vigilance to our mobile devices.


## TIP 5. ESTABLISH CLEAR CYBERSECURITY POLICIES

Crafting and disseminating a set of guidelines and directives on cybersecurity practices for your employees is important. While the specifics may differ across businesses, these policies typically encompass regulations regarding social media utilisation, bring your own device (BYOD) protocols, authentication standards, and more. Ensuring that your team members are aligned with these policies not only secures your organisation but also builds up a culture of accountability and awareness surrounding cybersecurity best practices.

## TIP 6. BACK UP YOUR DATA REGULARLY

Ensuring daily, or even more frequent, backups are important to mitigate the impact of data corruption or loss that could stem from security breaches. Adoption of a data protection tool, from your managed service provider (MSP),

which can facilitate incremental backups throughout the day is highly recommended. This approach significantly reduces the risk of data loss and builds up your defence against potential threats.

### TIP 7. ENSURE UPTIME

Selecting a powerful data protection solution capable of facilitating "instant recovery" of both data and applications is crucial. It's noteworthy that 92% of MSPs attest to the effectiveness of business continuity disaster recovery (BCDR) products in minimising downtime from ransomware attacks. Application downtime can significantly impact a business' ability to generate revenue. As we strive to maintain operational continuity, investing in such solutions is a strategic imperative for our business.

### TIP 8. MONITOR DATA LOCATION AND ACCESS

It's essential to recognise that the more places the data our resilience against potential breaches while safeguarding our sensitive information. exists, the more the risk of unauthorised access. Leveraging data discovery tools enables us to identify and securely manage data dispersed throughout our systems. Additionally, adopting business-class Software-as-a-Service (SaaS) applications afford us greater control over our corporate data, reinforcing our commitment to data security and compliance. By proactively managing data across our ecosystem, we enhance

### TIP 9. CONTROL EMPLOYEE ACCESS

Restricting employee access to specific data based on job requirements minimises the risk of insider threats. Grant administrative privileges only to trusted personnel to mitigate the potential for unauthorised access.

### TIP 10. ALWAYS STAY VIGILANT

Finally, the most important tip is to always remember that you're a prime target for hackers. Whether you're a small business owner or an individual, don't underestimate the risk by assuming, "It will not happen to me." Any digital device you own, whether at home or work, poses a risk if it can connect to another digital device. The probability of being hacked is consistently high. To stay secure, refrain from disclosing personal or financial information to anyone, whether you're a business or an individual.