VIKRAM SAREEN *Founder, Blue Bricks*
LinkedIn: www.linkedin.com/in/vikramsareen/

(Cybersecurity Expert, Multiple Patent Holder, Serial Entrepreneur, Board Advisory Member)
Vikram has over 22 years of experience in the cyber security domain. He holds multiple patents and has successfully commercialised multiple B2B Enterprise products. He has worked with over 120 BFSI enterprises, including banks and government bodies. In fact, his first work was used by then US President Bill Clinton to approve the Digital Act. He has a passion for problem solving, using technology, and is a regular speaker for discussion panels and events. Along with running his company Blue Bricks, he is also pursuing Ethical Hacking, Cyber Law and Cyber Forensics.

TIP 1. MOVE AWAY FROM EMAILS

The biggest emphasis by hackers is through emails where they encourage you to click in the message. Moving away from regular email to other team tools like Slack, Facebook, @Work or Microsoft Team will help your team to communicate much more safely. Also: create simple web forms for your customers to fill in for their enquires. Emails accessed on mobile phone are particularly dangerous as none of us install much needed protection.

TIP 2. JOB ROTATION IS MUST

Job Rotation means having employees switch their roles and work for two to three weeks in different positions. Security perspective is improved as any wrong doing, or escape routes, can be found - along with ensuring that each employee does not have complete control and become potentially dangerous. Please plan job rotations every six months at least. Also, do not give the same access to all your team members. Give MFA security tokens where you can, so it is harder for them to share their passwords with others.

TIP 3. USE GAMES TO SHARE SECURITY TIPS

No one likes boring training sessions, especially. for cyber-security. Games are the best way to engage to make it fun and better understood. Games can mean splitting teams as red, purple, blue with different roles to act out different physical and cyber scenarios. You can use Lego or Post-it notes as props. Trust me it is fun. Occasionally do cyber-security drill in the same way as regular fire drills as it will help a lot.

TIP 4. HACKERS LOVE BIG SECURITY COMPANIES, WHY?

No software or system is 100% secure. Even a 0.01% chance is enough to allow access. Microsoft, CISCO, VMWare, Remote Desktop (Citrix/VPN/VDI), Apple, Google, and hundreds of other large companies, are trusted by you and millions of others. Hackers love big companies as they will find vulnerabilities in this high volume popular software and exploit them; eventually they are causing you damage by stealing data and locking your systems. Go for less well-known, niche products that hackers do not know about. Governments do that, so why don't you?

TIP 5. HARD TALK ON FOMO VS JOMO.

If you have a limited budget amid ever-changing threats and a Cyber Security Officer is asked to protect your business, they will fail, for sure. Please don't go for FOMO (Fear Of Missing Out) or JOMO (Joy Of Missing Out) as neither will help you. Every company's security need is different to suit their particular culture and operation. You need to have an independent BOARD Advisor that is a cyber-security expert (who can guarantee you neutral and frank hard advice). Many companies select an Outsourcing Threat Monitoring Service - but they will never be fully integrated with your business's specific needs.

TIP 6. FIND A 'PARTNER' NOT A 'PRODUCT' FOR A LONG TERM FIX

The Bad, The Ugly and The Good are always catching each other in this hyper-fast cyber world; you might be ahead now, but not for long. We always think we have installed a suitable product and will be protected; this is a false promise to yourself. You need to have a partner that helps you with security needs over time. "It will not happen to me" is not a good mindset, you need to change to "It will happen to me and we need to review/fix it". A Partner that solves your problems over time, and again and again, is what is needed (products and services will become secondary).

TIP 7. PROTECT DATA AT ALL TIMES

Hackers want access to your data and ransom-ware is potentially extra cash for them; plus the fun in harassing you. Once they steal your data, then they lock you out. Data protection at rest and in transit (moving from user computer or mobile to server applications) is needed - so go for an application to protect that data. There is too much importance given to network security and antivirus but, sadly, none of them actually protect your data. If your data is protected, hackers will shy away as you are worthless to them. Ask your application provider to show you how encrypted data is stored. Don't settle for less.

TIP 8. JOINT ACCOUNTABILITY FOR "X AS SERVICE"

Online services can help us reduce cost; but it also comes with big potential headache. If Amazon AWS OR Microsoft Azure, Propertyme or Salesforce loses your data because of their system bug, they do not take accountability for their wrong doing. Most Software as Service systems that you use do not give you join accountability and data ownership. You need to demand them to be accountable for not sharing your data with other parties and to take responsibility in case any data breach happens.

TIP 9. WHERE IS MY DATA AND IS IT SECURE?

If you are going with cloud services, then data mirroring should be your key concern. We should, and can, use cloud based services but the data encryption is what you can control, so implement your own data security / encryption. There are good data protection tools that protect applications, files and data inside databases; most banks and payment companies use that already. This way, even your cloud provider mirrors (or backups up) your data, it is useless to hackers. No one wants to steal data as it then becomes useless and that is the best thing for you. Think of taking protection in your own hands, as no one else really cares for your data but you.

TIP 10. CYBER INSURANCE AND SECURITY ARE TWO SIDES OF THE SAME COIN

Your cyber security plan and rollout will give you direct benefits where you are not only protecting your users, applications, data and reputation; but you are also reducing your risk and, potentially, reducing your cyber insurance premium. In fact, most insurance companies demand you to have essential security in place in case you wish to claim. They will not force you, but they will surely reject your claim if you do not. So: best is to take security in your own hands for control, similarly to what you do for your car and home.