BHAVINI SINGH *IT Agile Business coach and consultant at Commonwealth Bank of Australia*
LinkedIn- https://www.linkedin.com/in/ratans-4b087921

Bhavini is a dedicated, and self-motivated, IT professional with over 13+ years of experience across various industries including: financials, consulting, healthcare and mobile and telecommunication. An analytically minded problem solver with a "think outside of the square" personality and a "can-do" attitude. Having an excellent track record in project delivery of a range of projects both at the enterprise and operational level in digital transformation, risk, compliance, and technology related projects, including cyber and infrastructure. She currently works at Commonwealth Bank of Australia as Program Agile Coach and Business Consultant. With her extensive expertise in cyber security governance, risk management, and compliance; she coaches the different quad how to establish cyber security strategies and processes across different platforms.

TIP 1. SECURE ACCOUNTS

Turn on Multi-factor Authentication (MFA) on your important accounts like email document storage and social media as MFA adds a layer of security to your account and protects your accounts from someone getting access. Protect your accounts from cyber criminals with a secure password or passphrase by using a Password Manager. Implement access control to ensure each user can access only what they need for their role.

TIP 2. DEVICE AND INFORMATION PROTECTION

Create and implement a plan to regularly back-up your information. Perform a factory reset before selling or disposing of business devices Configure devices to automatically lock after a short time of inactivity.

TIP 3. STAFF PREPARTION

Determine how cyber security awareness will be taught in your business. Create an emergency plan for cyber security incidents. Make an emergency plan and be sure that your staff are familiar with the plan, including any roles or responsibilities they may have.

TIP 4. DISASTER RECOVERY PLAN

Have a disaster recovery plan in place to help you respond quickly in the event of an attack. Consider how long it might take you to get back up and running after a significant disruption, so your business is not out of action for a long period of time. This could include how long it would take you to acquire new hardware and to restore your data. Your plan should include information on how you will communicate with customers and other stakeholders if their data has been accessed or lost.

TIP 5. THIRD PARTIES SECURITY CHECK

If your organisation's IT system is entirely managed by a third-party vendor, or supplemented by IT services provided by a third-party vendor, it is crucial to ensure that your vendor has clear cyber security and data privacy policies in place. Where you allow suppliers or contractors to access your systems, ensure cyber security requirements are built into their contracts and that their cyber security processes align with your own. If they outsource your work to another provider, check the outsourced provider's security processes and procedures

TIP 6. SEPARATE CYBERSECURITY FROM IT

Where possible, entrust cyber security management to a staff member who is not already responsible for IT matters. This will ensure objective consideration of security occurs when considering new IT services or extending existing IT services. If responsibility for IT and cyber security must fall to one person, consider having IT and cyber security as independent goals for that employee or contractor.

TIP 7. CYBER RISK CONSIDERATIONS IN BUSINESS PLANNING

If your business plan is focused on growth, you may need to add new platforms, products, apps and web capabilities. Cyber security considerations may multiply with the introduction of each new element. Align your cyber security protection plans to your business plan. This will help you identify and respond to emerging exposures e.g. third party and supply chain control deficiencies.

TIP 8. CYBER SECURITY CULTURE CULTIVATION

A robust cyber security system is not just the responsibility of IT but of each and every employee. Cyber criminals always find new ways to access information, therefore, it is crucial to create a culture where all employees are aware of, and understand, the impact of new cyber threats. You could invest a considerable amount in software to protect your business network only to find out that a simple error (such as an inadvertent sharing of passwords by a staff member) has provided provide access to cyber criminals

TIP 9. INFORMATION ENCRYPTION

If your business deals with data relating to credit cards, bank accounts, and other sensitive information on a regular basis, it's good practice to have an encryption program in place. Encryption keeps data safe by altering information on the device into unreadable codes. Encryption is designed with a worst-case scenario in mind: even if your data is stolen, it would be useless to the hacker as they wouldn't have the keys to decrypt the data and decipher the information

TIP 10.SECURITY POLICIES DOCUMENTATION

Once you have a protection plan in place for the business - which should include devices and network security best practices and what to do in case of a breach - it's time to get it all down in writing. Email a copy to all employees and post it in a common area for all to see. Have a meeting to go over every item and answer any questions or concerns. Check your policy every few months to make sure everything is up to date.