RAMAKRISHNAN SESHAGIRI, *Founder and Managing Director, CyberSafeHaven Consulting*
Website https://cybersafehaven.com

Ramakrishnan is enlisted in the National Security Database (NSD) as a Cybersecurity Scholar. He is a Certified Independent Director (issued by IICA, under aegis of Ministry of Corporate Affairs), a Fellow at Everable, and at Innovation and Technology Business Council, International Trade Council. He has over 25 years of experience in technology, primarily in product development and cybersecurity. He has multiple security certifications including CISSP, CISM, CCSP, AWS Security.

TIP 1. MAINTAIN AN UP-TO-DATE INVENTORY OF ALL THE COMPANY'S DIGITAL ASSETS (INCLUDING PRINTERS, ACCESS CONTROL DEVICES AND CCTV CAMERAS).

An accurate inventory will help every business maintain their assets in a secure fashion. If a CCTV requires a firmware update and this is not tracked as part of the inventory, the camera can be hacked, which, in turn, can have serious consequences.

TIP 2. HAVE A PATCHING STRATEGY

Most companies apply patches on-demand, based on criticality, or ask employees to update. The important thing here is to have a concerted strategy towards applying the patches, according to severity, complexity and the type of system. An urgent and critical update might need to be applied to a production server but what is the process to be followed for doing that without testing and disturbing the transactions?

TIP 3. TRACK USERS CLOSELY

The lifecycle of an employee's identity within an organisation, and the related credentials, are rarely monitored. A centralised identity management system, from which the access control to applications, devices and networks is managed, makes this task more manageable. Even in hybrid environments (cloud + on-prem), whether it is assigning or revoking permissions, adding MFA or moving the personnel to different departments needs to be authorised, logged and monitored since that has repercussions on the permissions that they carry with them.

TIP 4. ZERO TRUST PRINCIPLES

While identity management is one part of the larger jigsaw puzzle in managing overall security, defining the company's zero trust principles will help go a long way. Lost credentials have become the most preferred way for cybercriminals to tap into businesses' valuable resources without detection. Understand the other parameters that determine zero trust and define them.

TIP 5. TEST YOUR BACKUPS

Almost without an exception, every company is likely to say that they take backups. The critical question to ask yourself is, "are these backups ever tested?". The backups taken are of almost nil value unless they are verified and tested for further use. When disaster hits and you wish to recover from the backup and you realise that the backups are themselves corrupted, you have entered the realm of disaster exponential.

TIP 6. WHO'S ON YOUR NETWORK?

Guests, interns, external consultants, vendors and a host of non-employees are expected to visit your premises often. It is key to have a strategy to understand what access they need, and will have, to critical servers as well as Wi-Fi networks. Isolating the critical resources and allowing access only from certain networks will enhance protection.

TIP 7. ENCRYPT MOBILE DEVICES

Every mobile device, be it a laptop, mobile and other handheld devices that contain sensitive information, needs to be encrypted and preferably even controlled with a BIOS or a boot password. Devices are misplaced / stolen very often and this is the strongest way to protect company confidential documents and details from falling into the wrong hands.

TIP 8. HANDLING INCIDENTS

Every small incident needs to be handled appropriately. A server goes down for 10 minutes could be seen as a one-off event and ignored but best to record the sequence of events that led to the incident and how the recovery happened. This can be very useful in the future as your company grows and matures to handle incidents better and faster.

Destination: mch_seerver_host.
Product: GATEKEEPER SECURITY
Source: Internal phone host
CLONING CREDIT INFORMATION
TROJAN UPLOAD COMPLETE

TIP 9. HAVE A TRAINING CALENDAR

Cybersecurity is a landscape that changes almost every day, sometimes sooner. Given this, training the employees about the latest threats that they need to ward against - and what the company is doing for the same - needs to be planned. Ad-hoc sessions are fine but having a training calendar maximises not just attendance but also the effectiveness of such sessions.

TIP 10. PUT SECURITY BEFORE COMPLIANCE

It is always wonderful to be compliant with multiple standards like ISO27001 or NIST800-53 but please do ALWAYS remember that compliance can never lead to security. Higher levels of security can certainly lead to compliance. This thinking embedded in each employee within the company automatically secures the businesss to some good extent.