MOHAN MADWACHAR *Country Manager, Sattrix Information Security*
LinkedIn https://www.linkedin.com/in/leomohan/
Website https://www.sattrix.com/

Mohan Madwachar, a seasoned professional in the field of cybersecurity, holds a pivotal role as the Country Manager at Sattrix Information Security (SIS) Ltd. His extensive experience as a published author, speaker, trainer, and Cybersecurity Consultant further solidifies his credibility in the industry.

KYX is the Key to Your Organisation's Cybersecurity. Know Your Opponent (KYO), Knowing your adversaries is the name of the game. Whether it is your competition who wants to harm your business, someone from another country, or you are an innocent bystander caught between two other contenders. It is crucial to determine if you are the actual target of the attack or if they are trying to hack your website or extract information about your customers. You should also consider whether users act from inside or outside your Intellectual Property (IP).

TIP 1. KNOW YOUR CUSTOMERS (KYC)

Understanding your customers' business is key to building your organisation's cybersecurity. Key considerations include: how they transact with you, whether online or offline, how you store their data and financial transactions, and if they share their PII (Personally Identifiable Information).

TIP 2. KNOW YOUR BUSINESS (KYB)

If you are a legacy organisation transitioning to digital processes, it is important to understand how you conducted business before computerisation and how you operate now. Have you fully embraced digital technologies, or are you just starting your journey? Do you have a website that serves as the primary point of interaction with your customers? If so, do they share their data with you online, and if they do, how do you handle it? Is the communication channel between you and your customers fully secured? Finally, are you required to meet regulatory compliance? These are all questions you should consider to stay compliant and keep your customers' data safe.

TIP 3. KNOW YOUR INFRASTRUCTURE (KYI)

Your infrastructure has five important elements: Network, Users, Data, Applications, and Cloud. You need to consider how you operate, whether at your premises, remote, or mobile. You should also think about how your users connect to your corporate applications. Can you identify from where they are accessing your network? Are they using corporate-owned equipment? Are the endpoints secured to handle corporate communications? If you have developed the applications, have you followed the standard secure coding practices?

TIP 4. KNOW YOUR USERS (KYU)

Effective cybersecurity measures depend on user behaviour. Those who neglect cybersecurity hygiene become the weakest link in an organisation. Educate, enable, empower, and repeat.

TIP 5. KNOW YOUR ROLE (KYR)

The designations of CISO, CIO, CTO, and CDO come with great responsibility. Even a single data breach can lead to severe consequences and put the blame on you. Therefore, it's crucial to know your role, authority, powers, and responsibilities

in the organisation. You should document what you can and cannot do, as well as what you are responsible for and not responsible for. It's also essential to document any observations you make and communicate them to all stakeholders. This way, you can address any issues before they escalate and avoid negative repercussions.

TIP 6. KNOW YOUR VENDORS (KYV)

Original Equipment Manufacturers (OEMs) are responsible for developing modern cybersecurity technologies. Are they present in your country? Do they have a Technical Assistance Centre (TAC) and provide Return Merchandise Authorization (RMA)? Do they offer 24x7 support? Is the product stable and safe to install in your system? Are they committed to the locations where your operations are based? Is the product reaching its End-of-Life (EOL) or End-of-Sale (EOS)? Do they make commitments on the data sheet that they are unable to deliver? Do they have a long-term roadmap for this product line? Do they offer an integrated solution or just individual components?

TIP 7. KNOW YOUR PARTNER (KYP)

Whether you call them a partner, reseller, or system integrator, they are the link between you and the original equipment manufacturers (OEMs)! How do you assess their level of expertise? Do they have the necessary skills and experience to handle your project? How long have they been in the industry, and how stable is their organisation? Are they authorised to sell the products they offer, and do they have certified and trained staff? Will they be there for you when things go wrong? It's also important to understand their organisational structure and have a clear escalation matrix in place.

TIP 8 KNOW YOUR JOURNEY (KYJ)

If you have an unlimited budget, you might be tempted to bring in the best-of-breed solutions and pay heavily for them. However, if these components do not talk to each other, there will be no integrated management in place. This means you won't be able to understand what is happening in your organisation. Building a cybersecurity system is like constructing a house; each component needs to be synchronised, like the workings of an orchestra. If you ignore security, the digital journey becomes challenging.

TIP 9. KNOW YOUR FINANCES (KYF)

Budget and constraints are closely related. Out-of-turn investment requests after a breach may put a strain on your finances. It's important to anticipate these requirements and plan for them in advance. CFOs are always looking for ways to optimise costs and often target the Information Technology (IT) department. However, it can be challenging to explain the need for security tools like SIEM or SOAR to CFOs who may not be familiar with cybersecurity terminology. It's important to avoid using scare tactics like FUD (Fear-Uncertainty-Doubt) when presenting to top management, as this can lead to either unnecessary fear or dismissal of the issue. Instead, focus on presenting the information in a clear and understandable manner.

TIP 10. KNOW YOUR ACRONYMS (KYA)

PCMCIA - People Can't Memorize Computer Industry Acronyms! Just kidding! Often, vendors use acronyms while communicating. You should stop them if you don't understand them. IP and IP may represent two different things. One stands for 'Intellectual Property,' and the other stands for 'Internet Protocol.' If you are unsure about an acronym, don't hesitate to ask for an explanation. It's your right to ask and their duty to explain! Making assumptions can lead to wrong decisions. Sometimes, a conversation can be filled with acronyms for 30 minutes, and you may not understand any of them. You don't need to know all the acronyms or technologies, but it's your role as a guardian to ensure you understand what's happening in your company. That's important!