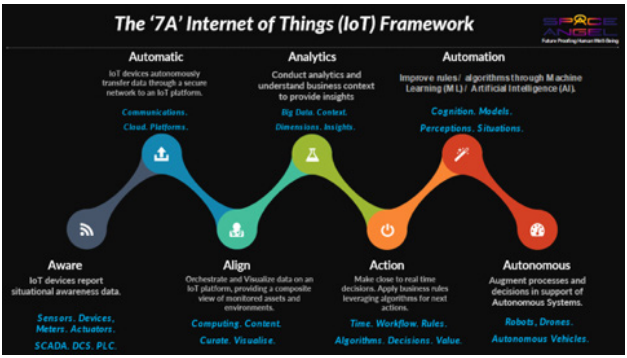
RAM KUPPUSAMY, *CEO & FOUNDER, SPACE ANGEL*
LinkedIn:https://www.linkedin.com/in/ram-kuppusamy-spaceangel-xcyber/
Website: https://www.spaceangel.io/

Ram Kuppusamy is the founder of Space Angel, a Communications, Command and Control (C3) company based in WA delivering next-generation digital technology and solutions for Space, Air and Earth; servicing critical infrastructure customers such as ports, utilities, medical, space and defence. Ram has spent 20+ years in ICT/ OT/IoT and has mastered strategy, disruption and transformation. In 2017, Ram won the ACS Digital Disruptor Awards for Skills Transformation of 21 to 200 people. He has produced a thought leadership piece on the '7A IoT Framework' envisaging a seven-stage evolution of IoT (Internet of Things) from simply providing situational awareness, to enabling full autonomy of smart digital applications.



TIP 1. STRUCTURE

Industries are rushing to replace manpower with robots, which showcases the importance of considering the cyber-security implications that come along with the implementation of these new digital technologies. Imagine a scenario at a restaurant where robots, which are connected through Wi-Fi, are serving food to customers. What happens when these robots are hacked by a cyber-criminal, act rogue and spill hot food on people? Who is to be blamed at this instance? Hence, it is important to embrace a structured approach to IoT security and we recommend using the 7A framework as shown above.

TIP 2. AWARENESS STAGE

This is the anchor stage in the IoT framework in creating situational awareness through sensors, devices, meters and actuators. The data collected through these devices generally goes through four stages, namely: Data at the edge, Data in motion, Data in Use and Data at rest. Due to the growth in different types of IoT devices, there is a need for close examination in determining the right cyber security strategies, given that currently there isn't one single standard for IoT. This "aware" stage is a very crucial part of the framework since it shows that security design considerations need to be incorporated at the beginning and not introduced in between. How well do you understand IoT standards?

TIP 3. AUTOMATIC

This stage is about communicating through various different types of communication networks and cloud-based platforms which require data to be sent and stored automatically in the cloud. Therefore, understanding the end-to-end solution architecture and how it flows through the enterprise with well-defined cyber-security protection practices and solutions need to be clearly perceived. Hence selecting the right solution, whether it is private cloud or public cloud or even Software-as-a-Service (SaaS) applications requires a good understanding of cyber threat considerations. How well do you understand your cloud environments and solution architecture? How mature is your cyber security practice?

TIP 4. ALIGNMENT STAGE

At this stage, data packets arrive within the IoT platform and are visualised in a meaningful format for interpretation. Device management components would include two types of devices: devices that just send data, or devices that control certain key functions; such as actuators, robots, automated guided vehicles, etc. Given this context, IoT platform security is absolutely crucial depending on the customer use cases and applications. How resilient are your encryption mechanism for end-to-end data packet encryption? What happens to your data if your AI robot gets physically stolen?

TIP 5. ANALYTICS STAGE

This "Analytics" stage is where data from an IoT platform, and other enterprise applications, are sent into the Big Data Lake. Data Lakes are flexible cloud-based environments which are typically used for the analytics of large amounts of data to derive insights. How well are your insights protected? In other words: how well is your IP protected?

TIP 6. ACTION STAGE

The "Action" stage is where all the IoT data, which has been analysed and insights derived, are used for business decision making to take in-field actions for operations. This usually includes the application of business rules and work flows. For example, the cyber-attack on the water plant in Florida reminds us that software used to take actions on critical infrastructure needs to be well protected. Question is how resilient are your systems that manage in-field operational actions?

TIP 7. AUTOMATION STAGE

In this stage, the opportunity for predictive analytics is presented by understanding the business rules from the "action" stage and introducing the application of machine learning and artificial intelligence algorithms, which leads to further automation of operational processes. How secure are your AI models and algorithms? How well do you understand the operational impacts and the business risk implications through the implementation of IoT?

TIP 8. AUTONOMOUS STAGE

This stage depicts, for example, the "Terminator or Star Wars" effect, which are basically smart autonomous systems that can make its own decisions and co-exist with humans. We might consider this fiction but this technology is currently around us through autonomous vehicles such as cars and trucks, which work alongside public road infrastructure. This not only poses potential cyber threats but can also affect human safety. Question is how ready are you to trust a smart autonomous vehicle, robot or device?

TIP 9. ASSET ACCESSIBILITY

With the world slowing moving into a digital era, IoT devices have become easier to purchase and install. IoT devices like smart lights can be found at your local hardware store. Therefore, it is imperative to understand where these devices are purchased from to avoid any future cyber threats. Ensuring that security measures are instilled from device procurement makes it easier to implement additional security hardening mechanisms to an IoT solution. This can be done by getting devices certified through International Certification Bodies while having a good understanding of both physical device security and software security. How do you select your IoT devices today? Do you know where it comes from and how secure they are?

TIP 10. APPLICATION

It is crucial to understand the type of applications to which a device is being introduced. If your IoT solution is for a critical business function, it is imperative to thoroughly understand the cyber implications associated with them. It is necessary to understand everything before purchasing something "cool" to add a benefit into your business, which might later end up in being a major catastrophe. Hence, we recommend the use of 7A framework which will provide a good methodology to provide guidance in relation to your IoT security strategy.