KORE

SUBJECT MATTER EXPERT (SME) INTERVIEW

IOT INSIGHTS REPORT:

IoT Solutions and Solution Architecture

With Bill Kramer, EVP IoT Solutions and Sunder Somasundaram, SVP of Pre-Sales and Solution Engineering

Bill Kramer serves as the Executive Vice President, IoT Solutions for KORE where he is responsible for developing, delivering, and supporting end-to-end IoT Solutions for enterprise customers. Enabling KORE to act as a trusted advisor to organizations navigating complex technology choices, Bill also leads KORE's professional services practice that includes consulting services and IoT endpoint lifecycle management services, among other management services that are designed to simplify and accelerate IoT deployments. Bill brings more than 30 years of experience in the data communications technology sector spanning wired, mobility, IoT, MMS, OEMs, and cloud technologies companies.

Sunder Somasundaram is the Senior Vice President of Pre-Sales and Solution Engineering where he oversees the IoT solution design and implementation process for KORE customers, focusing on ongoing sales and solution design success. Sunder brings extensive IoT experience to KORE, having spent more than 15 years at AT&T in leadership roles over both product and sales organizations. Most recently, Sunder served as the global head of sales for AT&T's IoT platform offerings where he was responsible for winning and delivering several large cloud and IoT projects.

Q1: What are the challenges most organizations face when they prepare to build an IoT solution?

BILL: The biggest IoT challenge most organizations face is that they lack the expertise and resources necessary to build a complete solution. They often don't know where to start and how to ensure success. That is largely due to the fact that IoT is still somewhat new and evolving rapidly. Knowing how to leverage IoT to improve business processes or operations is different than deploying traditional technology solutions.

SUNDER: Another significant challenge we hear from customers is the need to securely manage IoT solutions as they scale. There are many stories regarding inadequate security measures, including sensors misbehaving, bot attacks, and camera hacks. Enterprises deploying IoT devices onto their customers' premises are responsible for ensuring that the device does not become a vulnerability for the end user. End-to-end security is a key challenge for the industry overall, but especially for large-scale deployments.

Q2: Do IoT deployments increase in complexity with international or global requirements?

SUNDER: There are many challenges to consider with global deployments, particularly device certification and connectivity integration across different networks and carriers. For example, a global solution might need to work on a 2G network, a 3G network, and an LTE network. If the device is transported across any one of those networks, it needs to work seamlessly without any modifications to the device itself. That's a pretty complex problem all the way from integration needs to multi-carrier billing components.

BILL: I agree and would add that designing a device that works across all these different geographical areas and carriers becomes expensive. The device will have to support every band and frequency, and that drives up the cost. In this scenario, the customer could deploy one - potentially expensive - device that provides the seamless transition capabilities that Sunder described, or utilize multiple devices, each specific to a given region, as a more cost-effective option. So understanding these complexities and costs, and the ROI trade off, is important.

Q3: What are the most common mistakes you see when working with businesses on their IoT solutions?

SUNDER: One of the most common mistakes I see is the failure to determine an end goal. Many companies have vague goals that don't tie their IoT project to business outcomes.

BILL: Another common mistake is not having the right resources on hand to deal with the complexities involved with operating and sustaining IoT projects. There are industry surveys that indicate that 60 percent of all IoT deployments stall in the proof of concept stage. For the 40 percent that do get completed, only about two thirds of them are considered a success. So that means only ~26 percent (1 in 4) of all IoT projects attempted are considered a success.

We had one customer recently that was building an IoT-enabled product with strong market potential in its industry. The company researched the technology, but they lacked the resources to operationalize it. They needed external help to deploy, operate and sustain the solution, and successfully bring their product to market.

Q4: What are the required components of an IoT solution?

BILL: IoT solutions begin with an endpoint device, such as a sensor, that collects data. That data is transmitted through some mode of network connectivity, which could be licensed or unlicensed, such as cellular or LoRa. These components are managed by a platform, or multiple platforms, that handle connectivity management, device management, application development, security, and other functions. The data is then stored in either a cloud or hosted data center, where it can produce analytics or feed back office systems. There are many options for each of these components, making IoT solution architecture more complex than most IT solutions.

SUNDER: The way I look at IOT from a component standpoint is like a three-layer cake. At the bottom layer is the connectivity, which could be provided by a variety of options, even Wi-Fi. It really depends on the use case. The next layer up is comprised of two components: device management and the management platform. The devices and endpoints connect into the network, and the platform manages the devices and processes the data. The top layer includes the applications and data visualization, delivering the insights that result in business value.

BILL: There are two different ways to view an IoT solution and solution architecture. Sunder described a logical OSI stack perspective of the data and the solution, and what I described was an architectural end-to-end perspective. Both are relevant, and it is useful to look at them together to better assess your solution requirements.

Q5: Are some components or layers of the architecture more mature in their development than others?

SUNDER: While there is no such thing as 100 percent maturity in the constantly changing technology landscape, connectivity is the most mature aspect of the stack. We all have seen the buzz around 5G, licensed spectrum and unlicensed networks, which are still being evaluated for IoT. Still, I would say connectivity is the furthest along. Also, many of the cloud platforms have established standardized architecture, most notably from providers such as AWS, Azure, and IBM.

IoT device management is less mature. In IoT, there are literally tens of thousands of devices, each with its own operating system and protocol. By comparison, the handset world has just two dominate players - Apple and Android. Each is well established, making it relatively easy to manage these devices. For IoT, there is no single, mature device management platform handling these disparate devices. In many cases, businesses are running their own solutions to manage the devices on their networks. Businesses are also still figuring out the best ways to glean insights from IoT data.

BILL: I agree with Sunder, and I'll add that each of these IT components individually date back several decades. They are only immature in so far as they apply to IoT solutions.

Q6: Does the increasing quantity of devices, sensors, applications, and connectivity options/bandwidths make solution architecture more challenging?

BILL: Yes, and the lack of expertise and understanding of components is a significant obstacle for most businesses. With all the technology choices flooding into the marketplace, sorting through what's most applicable to your particular business process is very, very challenging for the average enterprise.

SUNDER: The biggest challenge is sorting through all the options. This is particularly true for global deployments with connectivity and device certification. Many organizations we've helped didn't even know that devices must be certified. They think it's as simple as buying the gateway and deploying the solution.

BILL: Technology choices mismatched to the application requirements have significant consequences. For example, I've seen an LTE Category 1 device selected and deployed for an application that required the bandwidth capability of a Cat-3 device. To put that into a quantifiable perspective, a Cat-1 device will drive 10 megabytes of data and Cat-3 devices will drive about 100 megabytes - so, it's about 1/10th the speed.

SUNDER: Organizations often don't fully understand the entire ecosystem of devices. So, working with an IoT partner, we can say, "That device isn't going to work. Here's another device that has a longer battery life," or maybe we can adjust the device to not report as frequently if battery life is more important.

Q7: How should companies approach building an IoT solution to ensure success?

BILL: It is important to look at IoT deployments holistically. Companies should think about all of the business areas they need to solve for, either internally, or externally. Thinking through all the critical capabilities needed for a successful IoT deployment – IoT strategy and readiness, application management and DaaS, as well as reporting and analytics – just to name a few – greatly improves an organization's chance of success.

SUNDER: Businesses across all industries are transforming, and this change is increasingly fueled by IoT solutions. Companies that were in the manufacturing business are now in the equipment management subscription business. A lot of our customers are pursuing new business models and IoT plays a key role in that transformation.

However, many organizations are struggling to build effective IoT solutions because they're not experienced in IoT – they're experts in their business. For example, as we mentioned earlier, there are literally tens of thousands of IoT devices, and choosing the right ones for any given application is a daunting task for those new to IoT. End-to-end IoT solution partners can help organizations think through the choices from a device perspective, from a security perspective and from a connectivity perspective to make the right choices for a successful IoT deployment.

Q8: How does a highly considered, strategic IoT architecture reduce deployment and time-to-market schedules?

BILL: ROI isn't achieved until the IoT solution is in the field and the intended business transformation occurs. Choosing the right technology for your business processes and strategic goals leads to operational efficiencies. These decisions are key to accelerating time-to-deployment.

SUNDER: First, identify what the end business outcome has to be, then put together the strategy. We don't even talk about devices, certifications or connectivity with our customers at first. We start with overall strategy and end goals, then work back from there.

Q9: Which internal stakeholders should be involved in determining business goals, outcomes, technical requirements, and timetables for an IoT solution?

BILL: It needs to be a cross-functional team. First, the business unit that owns the IoT business process should be involved to define needs. Then internal operations and IT teams need to get involved, as well as the finance team to do an ROI analysis.

SUNDER: The line of business owner needs to initiate the requirements, since they're closest to the problem and they understand its pain points on a day-to-day basis. They're looking for the solution that will help transform the existing business process. This recommendation should be presented to the CTO to make sure that it will be compatible with existing policies and security frameworks, then with the CFO.

Q10: Are there common events that trigger IoT experts becoming involved?

BILL: There are multiple points in an IoT project in which organizations may decide to reach out to external advisors for assistance. They may have begun, or already completed their technology selection, started the deployment and then failed. Or in some cases, they may have stalled and are seeking help in the deployment and operating phases. Ideally, an organization would begin with an IoT partner early in the process to help understand the business problems and explore the technology options.

The sooner a trusted advisor is engaged to help sort through the complexities, the better they will be able to align solutions to business processes and make technology choices for the entire lifecycle, through the deployment, operations, and sustain phases. We find that poor decisions in the early stages have significant repercussions in the later phases of the lifecycle.

Q11: If companies choose to partner with a provider to build an IoT solution, what should they look for?

BILL: The ideal partner isn't biased toward any particular component or vendors, has the experience and expertise to sort through the choices and can help businesses map the best technologies to their business requirements.

SUNDER: Businesses need to pick a partner that has a track record of delivering successful IoT solutions. Look for a trusted, neutral and expert advisor with demonstrated IoT knowledge and experience. To solve the holistic challenges of IoT, choose a partner that delivers complete, global IoT management capabilities to maximize ROI on IoT investments. An ideal partner will have the deployment agility to accelerate deployment schedules, and can solve the pain of multiple contracts with individual carriers, hardware/device vendors, as well as application enablement and service providers.

For more information, reach out to KORE to learn how we can simplify the complexity of IoT for your business.

info@korewireless.com • korewireless.com