HOW TO PLAN FOR IOT SUCCESS: STRATEGY AND RECOMMENDATIONS

The Internet of Things is quickly transforming how operations groups collaborate with IT in order to achieve better and more innovative business outcomes. But it’s important not to get caught up in the whirlwind of IoT hype and excitement; instead, organizations need to concentrate on how to plan, deploy and manage IoT use cases for tangible, quantifiable benefits.
When it comes to the Internet of Things (IoT), the numbers depicting its market impact are staggering.

- It’s a $737 billion market, reaching $1.3 trillion by 2020.
- The total global economic value of IoT technology could be as much as $6.2 trillion by 2025.
- IoT market expenditures are growing by 27% annually through 2018.

But as impressive as those and many other related statistics may be, they only scratch the surface of the exciting opportunity and potential benefits for businesses, public institutions and citizens around the world. That’s because IoT is really about finding new ways to connect people and things in innovative ways that result not just in more information, but better information. It’s a new way to deliver technology outside of the data center or other computing loci to operating points where it can do the most good.

The IT–OT Convergence

However, make no mistake about it: Successful IoT project deployment and ongoing economic value require careful planning, meticulous execution and the right tools. That’s because IoT is about the powerful marriage of operations technology (OT) and information technology (IT). And, like any marriage, there are potential pitfalls, challenges and complex decision points along the way.

One of the key steps in successfully marrying OT and IT is to let the operations team concentrate on what they do best, and to collaborate with their IT colleagues to ensure that things on the edge of the new network configuration operate more efficiently and effectively through well-managed and secure use of the latest data sources.

A vital element of the OT/IT marriage is the realization that the data center—literally and figuratively—is moving from its traditional environments into operating centers of the enterprise. It may be a factory, an operating room, a city intersection, an oil rig or a retail shelf that becomes the nexus of where and how data is captured, stored, managed, shared, analyzed and acted on. IoT use cases offer breathtaking insights into the technology’s potential to transform business operations for tangible benefits.
The Twin Challenges Of Security And Data Management

Among the inevitable and potentially daunting challenges of the OT/IT merger is how the hypergrowth of data—the vast majority of which is unstructured—impacts IT infrastructure, data management and security.

A recent IDG study showed that in 57% of the companies surveyed, security was the biggest challenge in their IoT projects.* Successful IoT programs are heavily predicated on identifying, preventing and remediating diverse and often-hidden security risks, considering the vast number and diversity of connected things. Security must be built into solutions to cover things like new endpoint devices, gateways, applications, cloud services and “factory/hospital/store shelf-as-data-center”-type models. This is a vitally important issue for IoT; after all, Gartner predicts that IoT security spending will eclipse a half-billion dollars by 2018, and that by 2020, more than 25% of identified attacks will involve IoT.⁴

Many early-stage IoT projects have revealed very quickly that these new programs cannot be accomplished simply by bolting on applications or dedicating individual servers and storage to IoT workloads. In fact, it requires an entire new way of thinking about—and implementing solutions for—such diverse requirements as data control, security, scalability, devices, connectivity and more.

The huge expansion of data volume, variety and velocity is putting tremendous pressure on IT infrastructure, as well as on operational systems. This data explosion and its challenges are personified in two major ways: data management and security. New paradigms are required in IoT use cases to ensure that data is managed for maximum efficiency, scalability, flexibility and adherence to next-generation data governance models.

---

*GARTNER SAYS WORLDWIDE IOT SECURITY SPENDING TO REACH $348 MILLION IN 2016,” GARTNER, APR 2016

---

| What specifically are/were the greatest challenges of this Initial IoT project for you? |
|----------------------------------------|----------|
| Security                               | 56.6     |
| Integration of devices (sensors/actuators) into the IT infrastructure | 49.1     |
| Development of a business model        | 39.6     |
| Analytics                              | 32.1     |
| Convincing company’s own staff          | 32.1     |
| Finding a suitable IoT platform         | 28.3     |
| Networking                             | 28.3     |
| Convincing Management                  | 22.6     |
| Convincing other departments           | 22.6     |
| Other challenges                       | 1.9      |

Multiple answers possible. Basis: n=53
The Criticality of the Control Plane

In order for IT and OT to work together seamlessly, securely and accurately, a new IT architecture is necessary. This IoT architecture is essential to control, manage and secure things, applications, data and processes from the data center to all operational centers of the enterprise. As a matter of fact, the IDG study revealed that the second biggest challenge in implementing their first project was the integration of the ‘things’ - sensors and edge devices - into their own IT infrastructure.

IoT architecture comprises two main elements: the content plane and the control plane. The content plane deals with data flowing from the edge of the system to the IoT platform—typically but not necessarily always in a traditional data center environment. Within this platform, data is sorted, analyzed and stored for analytics and a wide range of application requirements. This facilitates such tasks as predictive maintenance of non-IT equipment like oil rigs, injection molding systems and water treatment plants. It also is used in requirements such as supply chain automation and customer experience management, where the real-time and diverse nature of more and more data requires management of big data sets derived from both IT and non-IT devices.

However, it is the control plane that is often overlooked during the early stages of an IoT project. The control plane refers to the infrastructure, security and management required to implement IoT solutions, handling devices and non-IT endpoints from the edge of IoT system boundaries back to the data center or the cloud environment where IoT workloads may be hosted.
In the control plane, you need a “control center” to manage all things—both intelligent and “simple”—and to monitor their health and behavior. This should be implemented in the single-pane-of-glass paradigm very familiar to users of virtualization technology. Through this single management console, IoT systems can be securely monitored and managed, and services can be orchestrated for IT and business process automation, helping to reduce human touch points and freeing up both IT and operational personnel for analytics-based decision making.

Another important aspect of IoT architecture is the three-tier, or parent-child relationship. Generally speaking, enterprise IoT use cases have three major components: devices, edge system and data center. An example would be multiple temperature and lighting sensors connected to a gateway, all managed by an application in the data center. Most device management and enterprise mobility management products that exist today do not support the device parent-child relationship (e.g., “simple” sensors connected to a “smart” edge gateway). Therefore, new IoT management solutions are required to monitor and manage IoT infrastructure models.

Finally, many enterprise IoT use cases include remote, unmanned devices. This poses challenges for operations personnel. How will these devices be updated if the firmware is out of date? How can operations push a command to restart the device for troubleshooting purposes? How can the device be monitored proactively to understand when maintenance or replacement is required to minimize downtime? These are all critical requirements of the IoT control plane.
What To Look For In Solutions For IoT Today And Tomorrow

Organizations are running full speed ahead with IoT planning and systems development, and a blueprint is emerging for functionality and capabilities necessary to create real-world solutions. Among the key items your checklist should include when planning IoT solutions are:

**Support for diverse protocols**
There is a wide variety of things out there, each with their own protocols and data formats. An ideal IoT Management solution should provide vendor neutral management which is relevant now and in the future as standards and formats continue to evolve.

**Ability to orchestrate data**
As your IoT use cases expand, the amount of data produced by these will grow exponentially, and data minimization will become key. Your IoT management solution should be able to help you direct this data according to preset rules to minimize storage costs and have complete control of your data.

**Security by design**
IoT increases the surface area for attacks in your enterprise. Worldwide 62% of people cite privacy as a top concern with IoT while the average cost of a data breach is $4 million. Any solution you choose, should provide security at all levels of the device and data lifecycle.

**Automated detection/configuration/management of edge systems**
Monitoring, managing and securing millions of disparate things like sensors, devices or edge gateways on an ongoing basis is a challenge for an administrator. A good IoT management solution should allow automating activities like onboarding, pushing timely software updates as well as taking timely action on preconfigured rules to save time and effort.

**Scalability in building and deploying enterprise-grade solutions**
Supporting IoT use cases requires a change in the way organizations design their systems. You need a solution that allows you to not only manage both your legacy and new architecture seamlessly, but also be flexible enough to quickly add / reduce things to your systems effortlessly in real time to keep up with changing business needs.

Although this is likely to be the tip of the iceberg for IoT development, it is an excellent starting point for proof-of-concept projects, sandbox initiatives and pilots to test the efficacy of IoT for specific workloads in different industries. Over time, this list will necessarily expand to include support for diverse operational technologies ranging from kidney dialysis machines and IP-based video surveillance systems to interstate toll highways, aerial drones for package delivery and mobility-based voting booths.
VMware’s Approach To IoT Solutions

It should come as no surprise that VMware, an industry leader in cloud infrastructure and data center transformation, has positioned itself for IoT leadership. VMware’s expertise in infrastructure management and security enables it to provide an expansive framework for IoT solutions that is both ready for immediate business impact and provides a smooth runway for next-generation applications and use cases. In addition to building a new IoT infrastructure management platform, VMware has established a broad and deep network of partnerships with leading software, hardware and services providers to create a rich IoT ecosystem for customers. These partnerships are essential to achieving the exciting benefits of IoT because of the complexity and interconnected nature of IoT technologies, applications and processes. Among the key partners VMware has aligned with are Dell, Harman, ThingWorx, Deloitte Digital, V5 Systems, VizExplorer, Intwine Connect and Bayshore Networks, with many other partnerships anticipated in the coming months. This broad array of collaborations enables the development and deployment of value-driven business strategies, IoT applications and projects designed to enable the IT/OT merger.

VMware has already rolled out tools to help enterprises begin their IoT journeys, such as the Little IoT Agent (LIOTA), a vendor-neutral software development kit for IoT. LIOTA provides abstractions for the underlying IoT hardware system, the essential IoT gateways, attached devices, data analysis and data center connectivity.

This approach allows VMware to provide a single-source IoT solution based on four overriding principles:

- **Manage Broader**
  IoT solutions must enable the efficient management of millions of things just as easily as handling a single server or virtual machine.

- **Innovate Faster**
  It is vitally important that systems are designed, deployed and scaled as rapidly as possible in order to speed time to value for IoT projects ranging from proofs of concept to enterprise-wide rollouts that leverage early-stage learning and insights.

- **Protect Better**
  The vast and diverse footprint of IoT solutions mandates that organizations have the ability to keep the infrastructure system software operating at current best-practices level, isolate critical network segments easily, and deploy security fixes across the infrastructure in a timely manner.

- **Operate Smarter**
  A high-fidelity view of how various “things” are behaving is essential to spot at-risk endpoints, and it must be provided in real time with accuracy down to the device itself where an anomaly has been identified.
Conclusion

IoT may be the single biggest breakthrough in the entire technology landscape since the Internet, because it is poised to deliver substantial economic and operational value in nearly every business process throughout every industry.

Taking advantage of the groundbreaking potential of IoT will require a diverse mix of technologies, business process knowledge and services that bring IT into the realm of operational technologies. Because these solutions are complex and interdependent, success requires a single-source solution built upon a foundation of collaborations and partnerships across the digital spectrum.

VMware has already put steps in motion to enable the IT/OT merger through strategic partnerships, in-depth process knowledge and enabling technologies—with more on the way.