Industry 4.0: How to Overcome the Challenges of Supply Chain Digitization?

October 6, 2017 - **Neeraj Dharia**
Read Time | **5 Mins.**

Are you looking to digitize your organization using the Internet of Things (IoT)? Or are you a policy maker in the government who is part of the digitization initiative? Here are the four challenges you may encounter with digitization, namely interoperability, data security, job impact, and putting analytics to action, with suggestions on how you could overcome them.

[Gartner, Inc.](#) forecasts that 8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020. Total spending on endpoints and services will reach almost $2 trillion in 2017.

From the above statistics, it is clear that we are bulldozing our way to an 'IoT'ized world. You will notice that real-time shipment tracking is getting implemented across supply chains around the world and almost every mobile and fixed enterprise asset such as a warehouse or construction equipment is being tracked in real-time to improve its utilization or secure it. Every good change brings with it a set of challenges, and digitization is no different.

Here are four challenges you may encounter with digitization, and how you can turn them into opportunities as a user of IoT, a policy-maker, or a company providing IoT solutions.

1. Interoperability of devices

"I" in IoT stands for "Internet" and "T" stands for "Things." To enable the "Thing" to connect to the "Internet," you need a device you can attach to it, which will communicate to the web in real-time. IoT devices do not have standard protocols like your cell-phone. What this means is that the device you may use to track a shipment may not have the ability to connect to a WiFi network in the absence of a cellular tower.

On the network front, the SIM card or data plan you may use for your IoT device may not communicate across multiple cellular provider networks. How does it affect you? Assume you are using a SIM card provided by AT&T in a region where there are no towers of AT&T, but there are ample towers of T-Mobile that are present. Your SIM will still not be able to communicate due to the lack of interoperability between these networks. There are times when your cellphone's SIM may latch on to another telecom provider's network, during an emergency for instance, but it is not the norm with IoT applications.

How to overcome this problem?

As an IoT user ask your IoT solutions provider about how versatile their devices are – whether they will operate across telecom multiple networks, as well as across Bluetooth, WiFi, LoRA or NB-IoT.

A versatile IoT device and connectivity form two of the [5 most important aspects of ensuring your IoT success.](#)

If you are a policy-maker involved with digitization, develop standard protocols for IoT devices like those that exist with cellphones to ensure worldwide connectivity and emergency communication through a cellular tower that may not belong to the parent network.

If you are a telecom company, you can become a preferred IoT connectivity partner by offering to roam across other multiple telecom networks as part of your IoT plans, and also plan your cellular site locations with IoT applications in mind as against a pure population density based approach.

2. Data security

You are sending a consignment of high-value pharma goods to your customer. In the old days, thieves would follow your truck from the point of departure to the highway, and then find a secluded spot where they can corner and hijack your vehicle. You have now implemented real-time tracking on your truck to reduce your chance of theft, but does it reduce your risk? Or on the other hand, does it increase it?

If the data leaked out somehow and the thieves had access to it, they would not need to follow your truck from the point of departure and along the highway anymore – instead, they can wait at a secluded spot and await your vehicle to pass. See how the technology you implemented made it easier for the bad guys.

Such is the bane of digitization. Your sensitive information is running through the web in the form of codes and can land in the wrong hands if it isn't adequately secured. Sometimes, an employee in your organization could leak the information.

How to overcome this problem?

As an IoT user, you must invest in technologies like blockchain, ensure that your IoT platform provider is compliant with renowned industry regulations such as the 21 CFR Part 11, and ask for a customizable role-based access feature.

As a policy-maker, you can call for a compliance framework around security for IoT solution providers. The banking industry is an excellent example of how secure-access protocols are mandated through government policies for online banking. A similar level of involvement is needed for IoT enterprise applications.

3. Impact of automation on jobs

Automation's impact on jobs is a widely discussed subject where an 'MBA scholar' or a 'Company's senior executive' would say, "New types of jobs that will get created as part of automation will replace the old." What is not widely discussed by industry leaders though is the type of training that you need to provide to your employees and how to deal with change while going through digitization.

How to overcome this problem?

As an organization leader, you can successfully retain and grow your teams through the digitization process without letting go of them, while also increasing the ROI in the process by including the employee dividend portion in the digitization plan. You can build ROI by:
  i. Channeling new recruitment costs into training your existing workforce to skill-up.
  ii. Looking at new business opportunities with the excess workforce you would have otherwise let go of.
  iii. Gaining the good-will of the market by coming out as a skill-enabling firm – leading to lower costs and advertising at future hiring events.
  iv. Building employee loyalty (through skill-enhancement) which is a vital long-term dividend for your organization.

If policy-makers can create more awareness through case-studies and marketing ROI calculations on how automation and down-sizing are not beneficial to enterprises in the long-run, more corporate executives would be able to view the bigger picture.

4. Putting analytics to action

A client started monitoring fifty shipments every month, and every time they received a notification about their shipment deviating from the assigned route or when it stopped at an unauthorized location, they called the vehicle operator and instantly mitigated the risk. Once they scaled to over four hundred shipments, they were no longer able to take prompt action on the notifications - they didn't have the bandwidth. They knew what was going wrong but could not fix it promptly. This situation is commonly known as **"data deluge."** It is vital that companies create plans to address anomalies that may become visible upon implementing an IoT solution to avoid getting into a data deluge situation.

How to overcome this problem?

Setting up small control towers is one way to start. At Roambee, to help customers derive the benefits of an IoT implementation from day one without disruptive organizational changes, we

created BeeCentral, a "24x7 control tower" as a service concept. See how [BeeCentral](#) works.

There can be more challenges created by digitization, but these four being, interoperability, data security, the impact of automation on jobs, and the failure to put analytics to action are ones that commonly topple digitization initiatives across small, medium and large enterprises. Tackling them on the long-run is a joint effort between you (the user), policy-makers, and IoT solution providers. So, whether you are a user of IoT, a policy-maker or a solution provider, begin by doing your part today!

As part of your digitization initiative (to track shipments, packages, vehicles or assets in real-time), you need to explore a strong IoT solution to address interoperability, security, and putting analytics to action. Find out what constitutes a strong IoT solution!

roambee

Know More, Now.