



The Internet of Everything: A CEO's Checklist for Success

*A checklist to provide CEOs with the information they need to capitalize on the impact of the **Internet of Everything**.*



Richard Spangler, General Partner

3801 Beryl Road
Raleigh, NC 27607
www.plazabridgegroup.com
919.627.7970



The Internet of Everything: A CEO's Checklist for Success

Richard Spangler, General Partner

We already know the Internet is everywhere. We see it every time we check our Facebook feeds on our iPhones, browse the web with Chrome on our laptops, and access wifi hotspots in Starbucks with our tablets. It's obvious that we are growing increasingly connected. We're even seeing the spread of free wifi initiatives across the world. Programs from Winston-Salem to Singapore aim to provide citywide wifi for citizens¹, ameliorating their ability to maintain constant access to the world's "network of networks."

However, if we move beyond the existing population of iPhones, PCs, and tablets, instead focusing on the networks and interconnections of literally everything in existence, we start to realize the growth potential still possible for the Internet. The "Internet of Everything," for example, will change the way we interact with a variety of common appliances. Your smartphone may have an app that dictates your air conditioner always be set to 72 degrees. Your tablet may control your oven from afar so you can set it to pre-bake before you even get home from the grocery store. Virtually everything can become a communicating source, contributing information to the Big Data movement. With very little

¹ http://en.wikipedia.org/wiki/Municipal_wireless_network#Existing



extrapolation, we can see how the IoE will eventually reach bridges², roads, shopping centers, farming devices, and beyond.

Literally billions of new connected products are expected to — and will — be added to the Internet over the next decade. This enormous change will impact every CEO who delivers products and services to market. This impact must be understood and anticipated

if current companies want to survive the next great wave of innovation: the Internet of Everything Transformation.

IoE means that every device (emphasis on every) will have greater sentience and intelligence.

How can you prepare for this wave of change? How can your company get ahead of the storm rather than riding it out? First, you should watch for new product categories within your marketplace that are transformative.

IoE means that every device — emphasis on *every* — will have greater sentience and intelligence. This intelligence will then enable your product's autonomous operation and self-reliant serviceability. It will also change the business models behind your value proposition and alter the look, feel, and (more importantly) customer interaction with your product's value ecosystem. CEOs must begin, here and now, to examine how their product will change with the inclusion of machine intelligence and/or Internet communication capabilities.

Second, CEOs should prepare to manage the impact to customer privacy as if they were the Chief Privacy Officer of Facebook. (Yes, they have one.) Medical devices will collect personal health data³. Automated cars will collect location information, assuming your GPS

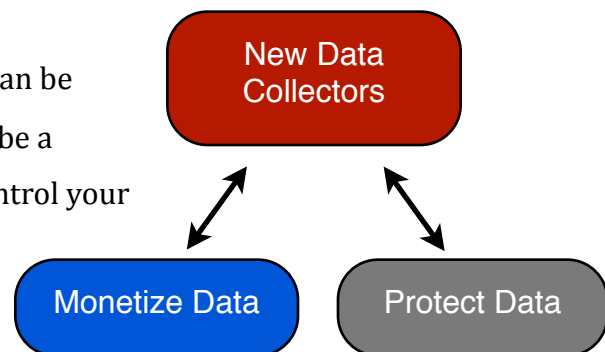
² <http://gigaom.com/2013/07/02/this-bridge-could-tell-you-when-its-about-to-fail-thanks-to-weightless-technology/>

³ <http://deviceprivacy.org/>



isn't already tracking your favorite routes. Cell phones will aggregate every detail of an individual's life from their contacts to their most personal secrets. In the same vein, you must ensure that you control the aggregated data from your products. One reason is that the monetization of data offers CEOs the opportunity to extract more profitability from their products. As we see margins from industrial products decline, adding new technology to the value of the resulting data is a path to margin protection and the establishment of competitive barriers. As a CEO responsible for protecting and collecting this information, you will need an expert knowledge of cybersecurity and personal information collection laws. This even applies to "legacy" industrial products. If your Dyson vacuum cleaner, for instance, collects usage information, then this means there are potential privacy concerns. The same will apply to your product.

If it is intelligent and communicates, it can be hacked. Once your product is in the field it can be a liability. Having a customer, or a third party, control your product in ways it was not intended can add legal risk to your bottom line. The damages of someone hijacking your industrial



switches, pumps, or machinery should be obvious. You must strategize risk management with a new perspective of aftermarket consequences. A great case study here is Cessna Corporation's approach to risk mitigation regarding their private planes flying well beyond their intended end of life. Because they were held liable for all their planes' costs, among other reasons, they discontinued their piston lineup. Via tort reform, they were able to restrict the number of years an aircraft manufacturer could be held liable for maintenance



or manufacturing defects. Since the reform, we have experienced a significant rebirth in aircraft manufacturing in this country. With the law, risk became calculable, which can now factored into the pricing strategies.⁴

Your company and its teams must then become experts on sensor technology. Much like the dynamic shift with the IoE, a revolution is occurring in physics and technology. New, amazing sensors are being developed that interpret light, measure discrete and continuous motion (human and otherwise), and advanced materials that act as receptors of data. Imagine being able to see where customers linger longest in your stores. Or noticing the wear and tear on your product simply by spotting the way light shimmies through its cracks and crevices. This plethora of new data collectors demands attention and innovation. Every product can benefit from sensor technology. If you aren't sure of the last time you spoke to a physicist, you should probably find one ASAP.

The IoE will not only make changes to your products, but also your product creators: your employees. A dramatic workforce shift will be required on your product teams. Engineering and product management teams must have the capability to include software engineering innovations, user experience advisors, and market strategists who understand the impact that technological innovation will have on your future products. The products will get more complicated and the teams must morph to incorporate new know-how.

You should also expect a new breed of thinkers to enter your establishment. With non-technical products going technical, new types of talent will enter your "normal" workforce. Folks that understand mesh networks, social media privacy policies, and cybersecurity protection strategies are a growing, traditionally-different breed. Ensuring

⁴ <http://www.flyingmag.com/blogs/going-direct/tort-reform-and-profit-margins>



the cultural compatibility of your existing team with this new workforce is your executive responsibility. While this is already top of mind for any leader, some preliminary planning may nonetheless be in the cards.

This also should lead you to understand how you must prepare yourself to include real, human employees in your product automation plans. We can already predict the growth of automated customer service and how it will soon intersect with intelligent products. The result will be the virtual elimination of the human element. That being said, products that should be able to fix themselves after an automated service call may not

Picture an underground gas pipe with a crack. Two automated machines can go back and forth until a stray cigarette ignites the leaked gas (and an entire city block).

exactly work as forecasted. Though the promise of intelligent devices should lead to all kinds of cost savings, CEOs must be prepared to keep the human element in the value mix. We learned from the call center automation craze that automation, when handled poorly, could damage a brand more than anything else. It is critical to have the “Press 0” option to speak to a human being even when your cable box should know how to “reboot” itself.

In your automation plans themselves you must also be on the lookout for “loops.” Intelligent products that communicate with your service teams, which have in turn already automated their response, can lead to closed loop processes that are difficult to detect, much less shield from the customer. Picture an underground gas pipe telling its service team that it has a crack. If the service response is automated, the two machines can go back and forth until either a service employee notices or a stray cigarette ignites the leaked gas (and an entire city block). Machine to Machine (M2M) communication can, in this way, lead to serious consequences that may not be known until larger problems arise.



CEOs should use the time now to prototype IoE ideas. You should start adding prototype innovation projects to your long-term product strategy immediately. Regardless if you manufacture industrial products, weave fabrics for clothing, or press plastic toys for the holidays, assembling a small team to innovate with intelligent sensors and communication capabilities will put you ahead of the pack.

The Internet of Everything

A CEO's Checklist for Success

1. Watch for new product categories within your marketplace that are transformative: IoE means that every device will have greater intelligence. This intelligence will enable autonomous operation and greater self-reliant serviceability.
2. Be prepared to manage the impact to customer privacy as if you were a Chief Privacy Officer. Collecting this information will require an expert knowledge of cyber security and personal information collection laws.
3. Ensure that you control the aggregate data from your products. Monetization of data offers CEOs the opportunity to extract more profitability from their products.
4. Remember: If it is intelligent and communicates it can be hacked. Having a customer, or a third party, control your product in ways not intend can add legal risk to your bottom line.
5. Engineering and product management must include the capability to include software engineering innovations, user experience advisors, and market strategists who understand the impact of technological innovation will have on your future products.
6. Become an expert on sensor technology. New data collectors offer the product manufacturer innovation on a silver platter. Every product can benefit from sensor technology.
7. Prepare to include people in your automation plans. We learned from the call center automation craze that automation handled poorly can damage a brand more than anything else. It is critical to have the "0" out option of talking to a human even when your cable box can "reboot" to fix itself.
8. Watch for "loops" in your product automation plans. Intelligent products that can communicate to your service teams, where your service teams have automated their response, can lead to closed loop processes that will be hard to detect, much less shield from the customer.
9. Expect a new breed of thinkers to enter your establishment. Ensuring the cultural compatibility of your existing team with this new breed is your responsibility.
10. CEOs should use the time now to prototype IoE ideas.