STARTING AND UNBLOCKING IOT WITH YOUR ECOSYSTEM

Kruijt, Menno and Bruininga, Andrew
COGNIZANT TECHNOLOGY SOLUTIONS

The potential of IoT is huge and so is its complexity. Therefore, this point of view aims to provide a solid understanding of the benefits and challenges of IoT for those in the corporate frontline of IT and Digital. Most IT managers find themselves struggling with full agenda's and big backlogs driven by ongoing digital transformation initiatives. It especially aims to guide IT managers and staffers in taking their first steps and preparing them for the exciting IoT journey in a comprehensive way. Amongst other things, it will shed light on the adoption of IoT amongst other enterprises and the challenges they face. Even more than other technologies IoT is a team sport. In football terms, on top of the first and second half it requires extra time to win the game with the help of coaching and specialized trainers. That is why it is important to understand your and your partners' capabilities to make it a success.

The IoT outlook looks promising: you claim your part

The potential of the Internet of Things (IoT) has widely been recognized by companies across the globe and cross-industries. Worldwide spending in IoT is likely to keep its double-digit annual growth rate until 2022 and surpass the $1 trillion mark in 2022 according to IDC (IDC, 2018). The sensor technology embedded within IoT devices are becoming more available, advanced and cheaper. As a result, Gartner expects the number of IoT devices worldwide to increase to 43 billion by 2023 (Gartner, 2017).

Yes, the IoT investment decision is a big one. And so is its trillion sized potential

IoT on the agendas: jointly adopt IoT with your new eco-system

A recent survey amongst 5.980 global enterprises (Ovum, 2019) show that below 30% of the respondents are currently deploying or have contracted to deploy IoT solutions stressing the huge opportunity highlighted before. Nearly half (44%) of the respondents that are already engaged with IoT, indicates that they see it as a core part of their broader digital transformation strategy. Half of the enterprises have seen measurable benefits from using IoT such as efficiency/productivity gains and worker/facility safety. Nearly 90% of enterprises expect to see benefits within two years of development. Over half of the respondents who began their IoT journey are running two to five IoT projects, whilst a third of the respondents have only deployed a single IoT project. Although, these IoT projects were relatively small with the majority managing less than 1.000 devices.

Smart homes

Cognizant developed an IoT strategy for a trade association. The problem statement mainly focused on what different roles the associated companies could take in an ecosystem for Smart Homes and how to get there. A quantitative and qualitative study had been conducted which led to multiple scenarios based on the adoption rate of Smart Homes and the potential fragmentation/consolidation of the ecosystem. With these scenarios in mind, Cognizant created three different strategies for the client to become a successful player in the IoT ecosystem for Smart homes.

However, IoT investments and device deployments look optimistic in the future. Some 85% of the respondents who are deploying IoT now are interested in running more IoT projects within the next few years. Another research conducted by Microsoft (Microsoft, 2019) amongst 3.000 enterprise IoT decision makers showed that 85% of the respondents have at least one project in the learning, PoC, purchase or use phase. A stunning amount of the respondents (94%) indicated their businesses plans to use the technology by the end of 2021. This begs the question; is the widespread use of IoT just a matter of time?

Reasons for IoT adoption

Grasping new revenue streams is often a main driver for starting IoT projects. However, Ovum's survey shows that only 20% of the respondents see this as their main goal, while most enterprises focus on efficiency, productivity, quality and cost savings. Driving opportunities for new revenue is considered more of a future aspiration than an immediate goal. Microsoft's survey results in similar reasons for adoption of IoT. The main reasons for adoptions are operations optimization (56%), employee productivity (47%) and safety & security in the physical world (44%). These are straightforward and let us now focus on what is stopping organizations from adopting IoT.

IoT is addressing classical business goals in short term; generating new revenue streams is a future aspiration

Challenges for IoT adoption

Ovum's survey suggests that data protection and management, and IoT security in general are the top pain points for enterprises deploying IoT. Some 40% of the respondents said "ensuring data, network and device security" was a key challenge. Furthermore, Data privacy/governance is also a big challenge for IoT adoption according to 31% of the enterprises. In addition, lack of internal IoT expertise ranked third amongst the biggest challenges for enterprises deploying IoT (29%). Coincidentally, resistance from line-of-business leaders/teams and gaining buy-in is becoming less of an issue within organizations (only 12% had chosen this as a challenge).

A survey conducted by Forbes amongst 502 executives who identified themselves as responsible for, or familiar with, the IoT activities of their companies had similar responses. IoT security was cited as a challenge by 32% of the respondents. Similarly, the availability of skilled talent (29%) and integration of disparate data (30%) was a challenge. Lastly, cross-department cooperation (31%) was seen as a distinctive challenge in IoT implementations from this research.

Similar results can be derived from Microsoft's research. Some 38% of the respondents have indicated that because of complexity/technical challenges they are not adopting more IoT. Lack of budget/staff resources (29%) and lack of knowledge (29%) follow next as barriers for more widespread adoption of IoT. At least 97% of the respondents have indicated that they have security concerns when implementing IoT, although it not being a hindrance to IoT adoption.

Microsoft's research also found that one third of the PoC's are failing. Predominant reasons being high cost of scaling (32%), unclear business value/ROI (28%) and having to justify a business case without short-term impact (26%). The latter reason for failure could be an implication of the agile transformation most enterprises find themselves in. Business value is delivered iteratively and incrementally in very short cycles of usually 2-4 weeks whilst most IoT projects give benefits only after 12 to 24 months.

Overview stoppers and blockers from recent research by Ovum, Forbes and Microsoft

The summarized challenges are lack of IoT expertise/knowledge, IoT implications on security (data, network and device) and Integration/governance of data.

	Ovum	Forbes	Microsoft
1	Ensuring data, network and device security	IoT security	Cross-department cooperation
2	Data privacy/governance	Cross-department cooperation	Lack of budget/staff resources
3	Lack of internal IoT expertise	Availability of skilled talent	Lack of knowledge

In agile terms: IoT is a significant epic, and it cannot deliver immediate value in 1 or 2 sprints

Framing security and see what is possible rather than what is not

On October 12th, 2016, a massive distributed denial of service (DDoS) attack caused a huge outage in internet accessibility on the U.S. east coast. The Mirai Botnet was the cause of this attack.

"The Mirai Botnet, targeted IoT devices – (...) that have been connected to the Internet, including wireless cameras, routers, and digital video recorders. (...). At its peak, Mirai consisted of hundreds of thousands of compromised devices. The defendants used the botnet to conduct a number of powerful "distributed denial of service" (DDOS) attacks (...) (Department of Justice, 2017)." [1]

These DDOS attacks proof the relevance of (cyber) security and risk departments. Historically risk management was considered as a blocker for innovation by sales departments. In fact, both departments were trading off reputation loss including regulatory fines and new revenues. Where sales department saw opportunities, risk management refused to sign-off since they were assessing too much risks using their risk framework. Driven by the agile movement and the ever-accelerating speed of new technologies, these frameworks have converted into "what-is-possible" scenarios as opposed to "what-is-not-possible" scenarios.

Companies in Microsoft's research that indi-cated that security was a concern for their IoT implementation have 3 to 4 security considerations on average. Collectively these can be divided into four main areas: device management (prominently on network and endpoint security level), software/firmware management (e.g., security protocols), training for involved employees and account authentications.

Framing the IoT security topic: what is possible (versus what is not possible) in managing devices (1), soft/firmware (2) and account/authentications (3). Training developers, product owners on security is a great starting point.

No one can play IoT alone: it is a team sport

Many enterprises have started IoT journey or expect to start it anytime now. The benefits of IoT have been widely recognized, but not yet achieved through full-scale IoT deployments. Mostly, because enter-prises are still trying out the technology with the focus on improving efficiency and saving costs through small pilots and PoC's. A vision and having business cases for (sub)deliverables in your IoT journey is fundamental to cross this bridge. Creating a vision comes with exploring multiple scenarios (see illustration "Smart Homes"). As enterprises and people gain more experience with IoT, there will be more focus on driving opportunities, generating new revenue streams or scaling their current IoT deployments.

Connected water

For one of our clients, utilities company, Cognizant had performed a gap analysis on the current capabilities in development, sales and support to implement IoT-enabled solutions. For this gap analysis, Cognizant developed an IoT assessment framework. A vision and strategy was created to protect future revenue, develop new data monetization opportunities and capture share in the Smart Home Market. Additionally, a plan was delivered to develop an in-house IoT capabilities focussing on connected water.

Integration and governance of data, IoT security and lack of IoT expertise seem to be the biggest stoppers now. If you encounter any of these issues, it is time to realize you cannot do IoT alone. Turn to trusted providers of cloud and enterprise IT services and solutions, with strong data/platform/cloud credentials to support your IoT needs. Every IoT implementation is different, in terms of requirements, outcomes, skills and technology required. However, there are five essential requirements for processes and practices that should be included in every IoT implementation (Cognizant, 2019).

It is crucial to identify the gaps within your own organization and create an ecosystem with complementary partners. Cognizant has developed an IoT readiness assessment¹ to help you understand your capabilities and support you in your IoT journey.

Solving your IoT impediments with your ecosystem

IoT is all about connectivity of its elements in its ecosystem. All team members need to play together in order to play (and win) the IoT game. It requires multiple departments and disciplines within an organization to build up an IoT ecosystem. The ecosystem involves market specialists developing new business and revenue models, IT associates mostly learning to reveal and link new data inputs, to operations professionals installing new sensors and refurbishing legacy systems to unleash historical data for analytical purposes. All department representatives must understand their role and must know how to deliver their parts in order to create the top line organizational value of IoT.
By default, IoT initiatives and decisions are crossing the borders of departments and even organizations. This is complicating the investment decision, which is again a team effort. Reality shows that the pre-match for IoT is an extensive one as it requires many buy-ins and alignments before the match-even can kick-off.

Navigating these challenges requires careful planning, domain knowledge and rigorous implementation. Based on our work with clients, we have identified **five essential requirements** for processes and practices that should be part of every IoT implementation:

1. **Edge computing/analytics**
2. **Data ingestion and stream processing**
3. **Device management**
4. **Cold path and advanced analytics**
5. **Enterprise integration with business systems**

Source: The Five Essential IoT Requirements and How to Achieve Them

To start with: shaping your IoT ecosystem to remove impediments related to security, compliance, technological complexity and data & device management

Getting started with IoT: all results give a competitive advantage

The synthesized results clearly show IoT is a hot topic on the IT manager's agenda and that enterprises share the same challenges. We are closing this point of view with a summarized advice for IT managers that want to prepare for their IoT journey or help those that have recently started. First, link real-life client problems with IoT solutions. Second, identify your capabilities and gaps with Cognizant's IoT readiness Assessment. This helps you setting the baseline and prioritize themes as an IT manager so you know what to focus on and where you need help. This is a crucial step in creating your IoT ecosystem to find the right partners that complement your capabilities. Third, structure and focus IoT ambitions and perhaps initiatives within your organization. Drafting your IoT team and ecosystem with complementary IoT partners and start a PoC is the fourth step. Once done, you are all set to transform the IoT PoC into a business project and deliver tangible results. Even bad results give you a major advantage over those stuck with IoT ambitions only. A famous scientist and one of the world's brightest minds once stated: "failure is success in progress".

Menno Kruijt is an associate of the Cognizant Digital Strategy Practise, based in Amsterdam, the Netherlands, where Andrew Bruininga is an associate director. Menno and Andrew are focussing on business value creation by leading-edge technologies such as IoT.

References

Cognizant, (2019, February). The Five Essential IoT Requirements and How to Achieve Them. 2019. Retrieved from https://www.cognizant.com/whitepapers/the-five-essential-iot-requirements-and-how-to-achieve-them-codex4241.pdf

Department of Justice (2017, December 13). Justice Department Announces Charges And Guilty Pleas In Three Computer Crime Cases Involving Significant Cyber Attacks. District of New Jersey.

Gartner. (2017, December). Forecast Analysis: Internet of Things — Endpoints, Worldwide, 2017 Update. Retrieved from Gartner.com: https://www.gartner.com/en/documents/3841268/forecast-analysis-internet-of-things-endpoints-worldwide

Gartner. (n.d.). Forecast Analysis: Internet of Things — Endpoints, Worldwide, 2017 Update.

IDC. (2018, December). IDC's Worldwide Semiannual Internet of Things Spending Guide Taxonomy. Retrieved from idc.com: https://www.idc.com/getdoc.jsp?containerId=US44652118

McKinsey. (2019, July). Growing opportunities in the Internet of Things.

Microsoft. (2019, July). IoT Signals - summary of research learnings.

Ovum. (2019, December). IoT Enterprise Survey 2019/2020.

Footnote:

[1] The assessment is available on www.cognizant.com/en-nl/iot-readiness. On top of the quick scan is an in-depth version available.

Cognizant