Things CEOs should know about IT

By Brad Barton, VCI Senior Consultant

As a modern CEO, the pressures surrounding the word 'digital' are intense. Shareholders expect better connections with customers and a more integrated supply chain. Frustrating inefficiencies in core processes seem like they should have been engineered out long ago. And what about some of the buzzwords? What is your company doing to leverage Big Data, Artificial Intelligence, and the Internet of Things?

This article is intended as a reference guide for CEOs on some of the things they need to be considering in terms of technology. Most organizations have a technology or IT department. They are often busy managing the transactional platforms for processes like HR and Finance and Procurement, as well as managing Cyber Security and SOX risks.

What should you as CEO do to make sure you're getting the most out of current technology investments?

1. **Make sure your technology function is a partner in your core business, not just back office processes and compliance.**

In this brave new world of digital awareness, it seems a shame if there's a dedicated stable of technology professionals that aren't focused on your core business. In many companies, IT reports to the CFO, and tends to be highly focused on transactional processes and compliance issues that are front of mind for finance.

Of course, not all CFOs treat IT this way, and having the technology function report into Operations doesn't magically cure the problem. In terms of structure, in terms of compensation, in terms of process, is IT pushed to be passionate about key business problems? When key decisions are being made, is someone from the Technology division in the room? Or (more ominously), do various business stakeholders avoid IT because of fears that their initiatives will be slowed down?

2. **It may be necessary to adopt a 'skunkworks' approach to get the technologists to think about things in a new way.**

If you have a technology division that's being avoided by key strategic initiatives, it's often not that productive to just send out a memo instructing everyone to involve IT. What are the core reasons for the hesitation? Bureaucracy? Speed to execution? A consistent 'no' rather than a thoughtful 'here's how'? Less than stellar digital user experiences on current tools?

Your IT department has had good reasons over the years to implement some of the processes that you may not enjoy dealing with. Without proper change management, system outages can occur much more frequently. Without early visibility from cyber security, problems can arise

that will scuttle a project, when they could have been addressed early. Support teams need to understand what's happening.

In spite of all of this, there are new ways of approaching some of these problems, but just telling a group of people entrenched in the old way to do it differently can be a tough sell. Sometimes getting a separate group together to work on some strategic work and pilot new processes can be a good way to go. The integration of the old with the new will still be challenging, but at least you've proven it can be done.

3. Target your data investments.

How many times have you heard the phrase 'we need to clean up our data'? I'm not suggesting that this is an incorrect statement. Getting efficient insights out of 'bad' data with no metadata and no hygiene can be extremely difficult.

However, if someone comes to you with a proposal that all data throughout the enterprise needs to be cleansed at the cost of millions of dollars and over the course of several years, you should probably ask some questions.

What are the insights we're after? Could we not focus our cleansing on a subset of data to prove the case? What safeguards are we putting in place to make sure that the same maintenance worker who identified the pump incorrectly doesn't do so again in three months?

Your company needs a data strategy and a roadmap to get where you want to go. Data cleansing will play a part. It just shouldn't be the only part.

4. Fundamental infrastructure updates may be required to leverage the latest technology, but make sure it's targeted and not just a repeat of yesterday's approach.

Most organizations want to leverage big data and artificial intelligence engines. Most organizations want to give employees, customers and other stakeholders rich experiences on mobile platforms. We watch our children writing code that results in reasonable app experiences, and wonder why our internal technology divisions can't produce similar wonders. Remember when the iPhone came out and our Blackberries suddenly started to lose their shine?

Problem is, big data and artificial intelligence engines are generally in the cloud. They require data aggregation and analysis. The neat drones you have doing equipment inspections produce an incredible amount of data to be consolidated and analyzed. It may be that you just don't have enough bandwidth on your network to do the job. You may not have the cloud architecture in place to make sure you've addressed the cyber security risks.

The trick on all of this is to do what's truly required, and what brings you into the future. Replacing every bit of gear in your old IT landscape with the newer version of that same gear doesn't necessarily get you closer to your goal, or I should say it's a very expensive way to get there. The cloud vendors are getting very clever with their Edge offerings, so not everything needs to be consolidated into the center anymore, but are your site server upgrades taking you in that direction or just reconfirming the old approach? Another example is that in some cases 5G can and should be used rather than another internal network upgrade.

5. **Cyber security risks are a real part of your business environment now.**

Just recently a bank's infrastructure was infiltrated, and millions of users impacted. Whether your company conducts e-commerce or handles customer financial records or not, the cyber security threats are growing and deserve to be handled as an important part of your business' risk register. This is a part of the balancing act of technology. If you empower cyber security to run everything and eliminate all risks, you will almost certainly have a technology function that finds it difficult to get things done. On the other hand, if you let the skunkworks get out of control and stop managing these risks, the damage to your business of a bad ransomware attack or personal data breach could be substantial.

At the end of the day, a well-run, traditional IT department adds value to your company, can help keep you out of trouble, and make back-office functions run more efficiently. But chances are there are some good ideas in the IT department waiting to help you in more meaningful ways. There is undoubtedly value to unlock in bringing your technology function forward onto more strategic projects.