Harvard Business Review

HBR Blog Network

IT Doesn't Matter (to CEOs)

By Robert Plant | August 15, 2013

In 2003 Nicholas Carr wrote a provocative article for HBR titled "IT Doesn't Matter," in which he stated:

"IT is best seen as the latest in a series of broadly adopted technologies that have reshaped industry over the past two centuries — from the steam engine and the railroad to the telegraph and the telephone to the electric generator and the internal combustion engine. For a brief period, as they were being built into the infrastructure of commerce, all these technologies opened opportunities for forward-looking companies to gain real advantages. But as their availability increased and their cost decreased — as they became ubiquitous — they became commodity inputs. From a strategic standpoint, they became invisible; they no longer mattered."

This argument was derided by IT supply-side executives such as Steve Ballmer, Carly Fiorina, and Scott McNealy, but CEOs quietly applauded it. They had suspected all along that IT really *doesn't* matter. Company leaders have quoted and lauded Carr whenever they've needed to justify their hesitation to create strong, progressive IT positions.

And they hesitate to create strong, progressive IT positions all the time. In fact, CEOs avoid IT like the plague. They resist getting their hands dirty alongside the CIO, even though many of them will readily get down into the mud of a balance sheet with the CFO or strategize the details of global brand issues with the CMO.

Because they distance themselves from IT, CEOs don't grasp its subtleties. Nor do they understand the CIO's role or, typically, the technologies that the company deploys. Consider the meager corporate progress over the past decades in easing two long-running headaches: enterprise-computing implementations and corporate security.

Even after more than 20 years of implementations, a study by Panorama shows that 53% of ERP projects still run over budget, 61% take longer to complete than anticipated, and more than 27% fail to produce the positive ROI expected.

And Panda Labs recently published data indicating that at a basic level, more than 27% of computers are infected with malware. Data breaches are on the rise, with a 44% increase in the number of records exposed from 2011 to 2012. There have been breaches at companies such as Global Payments (1.5 million records), Wyndham Hotels (600,000 credit cards), eHarmony (1.5 million passwords), LinkedIn (6.5 million passwords), Zappos (24 million records), Heartland (160 million credit card numbers), and even the Texas attorney general's office (3.5 million records).

Social media is now part of the security picture too: Between Q2 and Q4 in 2012 the number of Twitter accounts grew 40%, but the growth was accompanied by hacks such as those at The Associated Press, the FT, Human Rights Watch, France 24, the BBC, and Burger King. All of which reveal a deficit of security measures and a poor contextual understanding of the technology.

These and other IT-related problems aren't rooted in technology but in leadership failings. The people in the C-suite don't understand IT problems, don't provide adequate resources to solve them, and don't approach the issues as members of unified technology-literate teams.

To address these shortcomings, companies can take action in three areas:

> **Literacy.** The senior leadership needs to become literate in technology. IT isn't somebody else's job, it's ultimately theirs. Boards should require that CEO candidates demonstrate not just knowledge of finance and marketing but also a technology aptitude.
>
> **Accountability.** Boards should make CEOs accountable for technology failures and data breaches. The compensation committee should push for clearer links between pay and performance for IT-related activity (which ultimately is nearly everything most firms do). These links should be described clearly in the annual report so that analysts can scrutinize them.
>
> **Frequency.** The senior leadership group mustn't just pay lip service to the CIO and his or her team. The CIO's group is at the core of the business; it runs the company's nervous system (ERP) and immune system (security) and connects all internal and

external entities. Technology updates should be provided to the senior management team with the same frequency and rigor as financial statements and signed off on by the leadership team as part of the pay-for-performance framework.

It's true, in a sense, that enterprise computing is like a utility. Data flows through every company like water, gas, and electricity. But there's a difference. Computing's functionality undergoes constant, dramatic increases, and as it does so, it opens huge new opportunities and leaves the company vulnerable in unexpected ways. While technology can't give you a permanent competitive advantage, timely deployment of new IT products, processes, and systems can enable you to build a strong competitive position.

Corporations' technology strategies will remain ineffective until leaders acknowledge that, now as always, IT *does* matter.

This article was first published in the Harvard Business Review on August 15, 2013.
It is available online here: http://blogs.hbr.org/cs/2013/08/it_doesnt_matter_to_ceos.html