

Shadow IT: CIOs should use it as a Catalyst for Change

Businesses are under ever increasing pressure from their CEOs to deliver profitable growth but one of the mainstays to achieving this, IT, are not supporting them. To a more technology aware business community, who view IT as a constraint to them, the answer is simple - bypassing IT and procure, i.e. "self-serve", the technology solutions themselves. This has been made achievable by the growth of cloud-based anything-as-a-service solutions (whether this is software, infrastructure, network, DB etc.) and a more informed business who know what they want.

Interestingly the business doesn't perceive what they are doing as a risk to their organisation and would describe their approach to it as "getting business done now", a positive connotation. It's the very premise of Shadow IT: the business making technology work for them' whereas IT view it negatively - Shadow IT is a business behaviour that must be stopped as they are losing control. For the CIO is this a new challenge, or is it the same business and IT issues manifesting themselves in a different way?

The increase in "Shadow IT" can be clearly linked to the growth of cloud based solutions and digital consumerisation of IT (BYOD, BYOA etc.) and the unrelenting demand by the business for technology which they perceive to be better and cheaper than their own corporate IT function can provide and, more importantly, something that they can have immediately. Furthermore, recent research and surveys support this, with 80% of business and IT staff admitting to using non-approved SaaS apps, with 40-50% using them because they are familiar with them. Another interesting finding is that 24% use non-approved apps because they are better than the approved alternatives.

These facts highlight the problem that has been around for a number of years, the misalignment and understanding between IT and the business, and the failure of IT to deliver at the speed of the business. Interestingly Shadow IT is shifting the balance of power between IT and the business on who owns and procures the technology, and this trend is unlikely to be reversed in the near future. This view is reinforced by Gartner who predict that 35% of enterprise IT expenditures in 2015 will happen outside of the corporate IT budget.

There is also an argument that the organisation's Board have made life harder for the CIO and at the same time have inadvertently encouraged this behaviour by the business. In wanting to ensure that IT delivers value for money and demanding 'more for less', IT can't always respond quickly enough to the business's needs. So against a backdrop of budget restrictions, constrained resources, backlog of projects, tight governance processes and controls, and [instead of 'and' use 'combined with?'] its responsibilities and focus on security and maintainability, IT has gained the reputation of a function with a 'no' or 'come back later' culture. This is supported by research which confirms that about 40% of the business feels that IT is not responsive enough. On the flipside the business is under pressure to

drive growth and profitability so their only route is to source IT themselves. This is against [a backdrop of?] the global cultural trend of instant fulfillment driven by need and speed - technology on-demand.

Interestingly, IT is often perceived to have failed in delivering what the business needs due to poor management governance, business change etc. but who is measures whether business sourced and delivered IT has really delivered value [should this read: "... but who measures whether business-sourced and delivered IT has really delivered value?" ?]. The business will claim it's a success but they are not put under the same rigour and scrutiny as IT.

The challenge for the CIO is that the CEO holds them accountable for all IT related matters in the organisation, including data security and compliance, along with performance and availability. Yet increasingly the CIO is unable to control all of these aspects – so, for example, the boundaries of where corporate information is held is expanding from within the confines of the corporate network to out into the Cloud. The former is, and can be, controlled; the latter is often being? driven by the business and is unknown by IT – where are files held in Dropbox located? i.e., European sensitive data held in the USA. So the challenge for the CIO is how to be more open to the business procuring their own IT whilst still having the ability to monitor for, and protect against, any security violations, and also protect the business from itself.

Shadow IT also presents organisations with potentially significant corporate data security, regulatory and compliance issues, but for the business there is often minimal consideration for these potentially serious implications when they procure their own IT. Their main priority is to acquire what they want as fast as possible, but who is responsible and accountable for the corporate data, especially when there are data breaches or leakages - the business or IT? With Shadow IT, it is becoming increasingly difficult to ensure that corporate data is secure during its end to end flow – how many can say with any certainty whether their data has resided on non-approved cloud based solutions or apps, where

these are located i.e. USA, EU, Asia etc. and whether or not it conforms to regulation and corporate policies. This obviously increases the chances of a data breach and regulatory fines. How many know of the forthcoming EU Data Protection Regulation? This will include all the tracked information from mobile devices and that it will be mandatory for disclosure of a breach within 24 hours; the penalty of non-compliance is 2% of the company's global revenue.

Another result of Shadow IT that is often overlooked is the overall systems, and more importantly information integration. In the drive to adopt rapidly cloud based solutions how much enterprise data is being duplicated? How many data silos are being created? Where is the information being 'mastered' and how can the organisation know the accuracy of the information?

As a result of the fragmentation of IT across the business, the organisation is often unable to determine accurately the overall cost of enterprise IT and when they try to it can be a time consuming task. This leads to the next point that it also makes it difficult for organisations to ensure that they are optimising the value of their investments in IT.

So while there are currently perceived benefits to Shadow IT the reality is that it will create numerous issues in the future and become an inhibitor to growth. What is also clear is that it is another factor in creating a two-speed IT function, with one focus on the business cloud aspirations and another on ensuring that the legacy solutions (which either cannot be moved, or are too complex to move, to the cloud) are kept operational. Hence the rise of the Chief Digital Officer (CDO) to focus the technologies that will drive business growth – cloud, collaboration etc.

If Shadow IT is not addressed jointly by the business, IT and the board, then the business divisions will continue to procure cloud solutions and, in some cases, infrastructure until each has its own IT function. This means that the ownership and governance of technology will

fundamentally change shape – from a single IT department silo to many line-of-business technology silos.

There is now an opportunity for CIOs to use Shadow IT as the catalyst to consider what should be the overall role of IT in the organisation, to rethink a number of the key principles of how enterprise IT is delivered, now[how?] to align it to the emerging digital trend and enhance the working partnership with the business. In essence CIOs need to embrace the principles and drivers behind Shadow IT to ensure that IT doesn't become totally fragmented and dysfunctional. If they don't, they will just be left with the legacy and operational elements, becoming a support function with no position on the board – the new CDO will take that role.

In considering IT as an ecosystem with elements that may fall both inside and outside the existing IT function, how can the next generation enterprise IT be delivered? There are different options to assess when rethinking how to deliver IT: as a service ("IT-as-a-service") model – where it creates an environment where IT adapts to support current practices, current business needs, incorporates new and different technologies and makes it all work seamlessly - or as a decentralization model, moving certain IT responsibilities into the business – maintaining 'corporate' critical elements and devolving 'local' non-critical components to the business. IT must define and maintain the framework of how the business can operate i.e. managing the standards for governance, compliance and regulatory, security etc. The latter [model?] is already happening with Shadow IT, but the difference is that it is putting it on a formal basis. By accepting responsibility the business will also be accepting ownership and accountability.

With the advent of these challenges CIOs need to recognise that they must expand the breath of capabilities to encompass advisory and integration specialists in order to deliver the evolving enterprise IT. They should consider: Technology Brokers who can provide buying advice and negotiating support to divisions across the organisation to ensure procurement decisions are sound and that technologies are

compatible with existing systems; Cloud Integration Specialists who are dedicated to addressing compatibility and integration issues, as well as working with the business users to ensure the solutions are fit for purpose; and Business Advisors, who are seeded into the business so they really understand their challenges and can play a consultative, challenger role to ensure the next generation IT truly integrates business, information and technology together to create the necessary increased flexibility and responsiveness.

The CIO needs to reposition, and rebrand, both themselves and their IT function to ensure that they are seen as the catalyst for growth of the organisation, but there is a decreasing window of opportunity for them to do this. During this dysfunctional period they need to evolve IT rapidly into a new hybrid model, strengthening the centralisation of core critical IT elements and devolve those that could, and should, reside in the business.

So the "Next Gen CIO" will need to focus on being an advisor and integrator and not just a developer and operator; will need to manage the prime corporate asset – information - and not on delivering and operating systems, servers, networks; will need to refocus on business productivity and not process standardisation and efficiency; will need to encompass proper risk and compliance management including internal; and will need to transformation[transform?] their function to embrace the new digital opportunities. Otherwise, the business will grasp the initiative and leave the CIO with the role of just "keeping the lights on".