Bridgeway

CIO
Conversations

Former CIO and CDO
Jos Creese has over 30 years
IT leadership experience.

Treading the digital transformation tightrope: how can you be a successful CIO in 2019?

Bridgeway chats to Jos Creese

We caught up with top digital transformation influencer Jos Creese to discuss the current challenges that many CIOs face. Jos has over 30 years IT leadership experience, including CIO and CDO roles, and a variety of Non-Exec Director positions (including audit, risk and chair). He is a past president of both the Society of IT Management (SOCITM), the BCS, the Chartered Institute for IT, and has been cited as 'the most influential UK CIO' in the Silicon 50 survey.

For over a decade Jos was CIO and latterly CDO for Hampshire County Council, leading a range of ground-breaking shared services and achieving national recognition with a host of awards for IT innovation. He also set up and chaired the Local Public Service CIO Council and worked with central government on a range of national programmes such as open data, ID cards and national supplier contract negotiation. Jos now works as an independent consultant, researcher and Strategic Adviser to Advice Cloud providing expert advice to public and private sectors on digital and IT strategies. In this interview he chats to Bridgeway Content Editor Lisa Higgins.

Hi Jos, let's kick things off with a question we are always interested in. In your opinion, what are the biggest challenges for CIOs at the moment with respect to digital transformation in the public sector?

Hi Lisa. For CIOs the biggest challenge is balancing the risks and legacy constraints around technology with the excitement and enthusiasm about the new order of digital delivery.

Say you have a departmental head, a Chief Executive for example, desperate for some new level of customer self service automation, or artificial intelligence engine to revolutionise a service. Such tech may deliver better customer service or move the organisation forward around productivity and efficiency, for example. The CIO has to grapple with the underlying platform that already exists – the technology infrastructure and security access management support. He/She cannot necessarily just decommission elements of that legacy in order to release the capacity, staff and money to pay for the new stuff.

So there's a sort of political challenge here as well as a business and a technological challenge for CIOs in helping to explain and support the migration to a new operating model – the digital transformation piece – in such a way that doesn't expose the organisation to undue risks, or indeed costs, especially in a transitional period.

So it's quite a complex issue, then?

Well it certainly isn't just, 'there isn't enough money' or, 'how risky are these new technologies?' Tech has always had its risks. The best CIOs are working at board level to help their organisation close the gap between the potential of some of these new technologies and the business opportunity that exists. And that's true of public and private sector.

According to last year's Deloitte survey CIOs have moved from being trusted operators to business co-creators and change innovators. Would you agree and how has your role and mindset changed since your first CIO role?

I have seen the Deloitte survey and I only partially agree with that statement. If you talk to any competent CIO they will say, 'absolutely, I am a co-creator and a strategic resource. I'm not just an Operations Manager,' and of course many of them are definitely of that ilk. Many are working at board level helping to formulate their organisation's business strategy. But we've also seen organisations where that doesn't happen and they have come a cropper in terms of significant information data breaches or system failures. TSB is an example here and chief executives lose their jobs if they fail to understand the risks and opportunity. So there is an element of truth in the survey.

However, what I see on the ground in both public and private sector is that in some organisations the culture still exists of IT as a cost centre, responsible for managing operational IT matters, a responsive and resilient infrastructure, manager of IT suppliers and so on. In parts of Whitehall, for example, some CIO responsibilities have been relegated to what I would call a more traditional operational IT management function.

So I think it is quite mixed actually and it is not all to do with the competency and attitude of the CIO themselves. It is often to do with the culture and the maturity of the organisation in understanding the potential of technology as a strategic component of services, rather than an operational contributor.

Who do you see as the trailblazers in the public sector?

There are plenty, particularly some of the bigger public service organisations such as Leeds City Council, Essex County Council, Cambridgeshire County Council and Norfolk County Council. Aylesbury District Council are also very ahead in what they are doing.

The leaders are those that have highly competent and innovative CIO's who are able to juggle not just both the legacy and traditional IT management with the more strategic outward looking digital agenda but also the organisation politically. You can have organisations where the CIO is more than capable of doing that but the leadership just don't really get it – they don't want the Head of IT to take on these responsibilities, they want to give it to the Transformation Manager or they think IT should be about just keeping the lights on. These organisations hold themselves back.

Is that kind of attitude the biggest resistance, in your opinion?

There are a number of barriers. A lack of change leadership and a lack of seeing IT as a strategic resource in a digital operating model is an issue. You see organisations say, 'we wish to be a public sector digital business providing public services and we want to be a digital leader,' but then you look at the evidence and discover that: a) the corporate strategy has a bit of a bolt-on about digital at the end, b) there's no detailed digital strategy just a set of digital programmes that will hopefully connect together to deliver some of this stuff and c) completely separate and relatively unrelated is an IT strategy plan which is primarily focused on how to keep the legacy going.

This is a major problem. What you want is a digital strategy which courses across the whole of the corporate strategy and business plans and is used to drive IT prioritisation and activity as well as investment. This is so that the digital strategy gets the appropriate investment as a result and equally IT is expected to contribute in terms of potential opportunity and innovation back into that digital strategy and corporate strategy. When you get that sort of synergy then you have a very effective organisation. Inevitably the bigger tech companies do this because tech is their bread and butter. But when you're not a tech company, when you're a police organisation or a health authority or a local council, you have to work harder to make those sorts of connections, particularly to understand and manage the risks and especially in a political environment such as Whitehall and local government where you've got politicians representing the interests of the public.

Is it therefore about empowering the IT department to be more aligned with the business heads and have more of an active role, giving IT a louder voice?

Well it has to be a two-way street. I see Heads of IT and CIOs that make the case in the wrong language to their business colleagues. They use a lot of jargon and they talk about the excitement of machine learning and robotic process automation, for example, without explaining how it will impact on outcomes. They talk a lot about risks, concerns and vulnerabilities which means that the organisation could not tolerate certain elements of mobile and flexible working or partnership integration without lots of controls being in place. But they don't paint a positive picture around all that because they see themselves as auditors, police controllers and regulators to protect the organisation from itself. But these are not good traits for business leaders in IT.

The CIO has to be the buffer between the business and their own teams. You've got to have people who do worry about those risks but equally the CIO has to be able to moderate them. Many of the technology risks that we see in some of these new solutions available in the marketplace are business decisions not IT decisions, yet sometimes IT thinks the business isn't capable of understanding or making those decisions so they think they should do it for them and ban BYOD, for example. They stop certain things happening because they make the assumption that the business is not ready, can't afford something or shouldn't be allowed to take the risk because something horrible will go wrong.

It also lends the other way. How do heads of legal, procurement, chief execs and exec leaders generally perceive the role of technology solution providers both internally and externally? Do they all understand what cloud adoption actually means? Do they understand what the risks are, what they should expect from IT and how they need to support IT? And that is not just with money but in terms of the support from frontline staff in being vigilant for phishing attacks or whatever it might be.

So how then would a CIO measure the impact of technology to the overall business performance?

Great question. They often don't do it terribly well. There are obviously some traditional metrics such as the SLA type measures that look at how often the network goes down, how many interruptions there were, how quickly IT fixed things, how many problems IT solved, etc. But they are often proxy measures and not very good ones.

If you take help desk, for example. Traditional help desk metrics would look at: how many problems did help desk solve this year for XX amount of money? And they may conclude, 'this year we sold many more for less cost.' Well that is the wrong measure. The way I would measure is to create a dashboard of business metrics related to digital operation and IT investment designed and fulfilled with the business head. You would go to the Director of Finance and ask, 'what are the outcomes that you expect? How would you measure the success of IT in your area, compared with similar industries, based on the priorities that you set?' Those measurements will likely be very different measures to what IT measures against by looking inwardly at itself. You would then end up with a series of business dashboards based on the main corporate priorities of the organisation that would be real indicators of corporate success around IT delivery.

The challenge that comes with that is then you have multiples accountabilities. Of course many organisations will be concerned about this as it implies matrix management and potentially diluted accountability. It sounds problematic but actually it is the way forward.

If you've got a digital programme, you need a common way of doing certain things across a whole organisation and a collective responsibility. I do see organisations doing this successfully. A social care organisation might say, for example: 'Nobody is going to get a bonus this year. No one has managed to succeed in their own performance targets not because we didn't deliver a really good social care to children, we did really well on that this year but the organisation has not been able to fulfil it's ambitions around purchase to pay', (which would be a process that tackles the whole organisation including the allowances for children's social care). Therefore everyone is marked down'.

In other words, you need to create a collective responsibility that allows directors and the CIO to be accountable for and involved in a multipolarity of digital development.

So it's a different way of working – does size matter here?

It's much easier in a smaller organisation. An SME works this way all the time but in a big complex public service or corporate organisation, it's much more difficult to do. We have built up a whole infrastructure of compartmentalising in order to manage the risks and performance and in a digital model you need a different way. The idea of corporate service, for example, doesn't exist any more in the traditional way. Yes you might still have procurement, legal, finance, etc but they become cross cutting roles with business account managers and strategic thinkers embedded in the organisation while also operating corporately.

What staffing and skills challenges do you foresee in coming years?

That's a good question as well. With regards to staff, I see significant challenges on the horizon. There are the traditional ones – there's a global skills shortage, we're still turning out traditional skills that are not always fit for purpose through some of our education systems, and the public sector in particular has a whole range of problems around ridiculous pay constraints for IT professionals which means it's particularly hard to recruit and retain the best people. There's a starting point.

The particular skills we are lacking? Well what we are seeing is a sea change which is going to be very evident in 2019. We've seen a major and continuing fall off on traditional outsourcing. Many public service organisations in particular have followed a mantra, often politically driven, that says, 'we don't want to run IT anymore, we'll just get the private sector to do it so we'll give it to Capgemini, Capita, Accenture, avato, etc. because this will create innovation, cost-savings and greater flexibility than we've had from our own in-house team.'

What that has resulted in is higher costs, inflexibility and some major constraints in moving to digital. To be fair to the outsourcers they are all beginning to try and change what they are doing but those traditional models are being replaced with, for example, cloud based solutions.

What do you see on the ground?

I'm working with a lot of organisations that are struggling to eradicate the constraints of legacy IT in their outsource arrangements and want to bring stuff back in house. I'm not convinced that it is the right thing to do but certainly the migration to cloud implies some new skills are going to be required and I think those skills are a new style of IT supplier management. If we are going to move more stuff to the cloud, the risks and the management constraints around off-shore processing and management of data will be important, so how will we manage that?

I also see some in-house skills required in terms of a new style of platform design and there are specific areas such as cyber resilience in its broadest sense. This is not just IT security but how we ensure that the organisation as a whole has got sufficient resilience protection against a range of cyber risks. For local authorities this includes emergency planning and business continuity;

a major technology digital infrastructure incident in an area might not just affect the council, it might affect lots of partner organisations and indeed the public as a whole.

There is a civic responsibility for councils to get involved in those sorts of things and there is some major work going on at SOCITM with this at the moment in helping to define how councils in particular should work with police, Whitehall, National Cyber Security Centre etc. But to do this you need a level of in-house skills at a sufficiently high level to maintain the appropriate partnerships and strategic understanding.

We are seeing a growth in low-code/no-code type development. While that implies you don't need to know anything, actually you do need to know something and the way of exploiting those sorts of new technologies will be important. There are risks around AI and how that could be introduced, and new styles of IT strategy which resolve legacy constraints and can exploit new technology without the appropriate risk of cost. All these things are going to put particular pressure on the skills required for IT leaders and their teams. I don't envisage a mass move to in-house and building up the traditional IT empires of the past, but I do see a need to ensure we have got the right level of in-house skills for some of these activities.

In your opinion, what are the biggest concerns for the CIO when it comes to cloud security?

Generally the IT managers I talk to are not scared of cloud, they see it as a major opportunity. Most of them are using it in some way or other but the adoption of cloud does bring with it a number of concerns. One is trying to avoid a patchwork of cloud solutions – you have a myriad of optimised cloud solutions but the ability to join them together is a major headache. There are concerns about the competency of some suppliers, not in terms of the particular product they are selling, but in terms of the cloud platform that they are running on: How secure is it? How well is it being maintained and managed? There are concerns about costs because the earlier cost saving predictions that we heard from many suppliers have not been fulfilled at all. And some of the big cloud suppliers look a little bit as though they may become monopoly platforms and as such can we expect to see them starting to become more expensive? It's a worry.

Also given the legacy concerns, IT professionals need to manage a transition to cloud which requires new IT policies, IT strategies, skills and the ability to manage a disparate access management and IT security environment. Migrating to the cloud will require relatively sophisticated data testing and master data management to be in place.

For these reasons quite a few organisations are opting to develop and maintain on-premise cloud or hybrid cloud solutions until some of those issues can be resolved. Sometimes this can look like inertia, being risk averse and/or not cloud ready, but actually there are some good practical reasons why complex public service organisations don't simply say, 'let's just shove everything in the cloud tomorrow.' It's planning, getting ready and being sure when one member of your department says, 'we want to move this and we want this new system and it's only available in the cloud' and you can say, 'OK, absolutely fine, we can move this to the cloud, but does it conform to our data management policies that the executive team have endorsed to ensure that data is held securely and safely, that we can get it back when we want it, we know where the risks lie and who the data owner is?'

You need to make sure that you are finding the right solution and indeed have a personal accountability particular around GDPR to ensure that any services that you adopt in the cloud will conform and comply with your requirements – and these are corporate requirements not IT requirements.

We'd like to thank Jos for sharing his insights with us.

Bridgeway

Bridgeway Security Solutions Ltd.
Bridge House, Anderson Road, Buckingway Business Park,
Cambridge, CB24 4UQ, UK

T: +44 (0)1223 979090 E: info@bridgeway.co.uk

www.bridgeway.co.uk

About Bridgeway Security Solutions

Bridgeway is an information security and risk management specialist with proven experience in delivering security solutions around mobility, cloud and security intelligence.

Bridgeway offers a holistic approach to understanding business issues and matching superior solutions through our depth of marketplace understanding, consulting expertise and using trusted vendors to deliver sustainable advantage. Our vision-led approach takes products, policies, processes and people into account, helping customers overcome security and risk challenges and enhance their business.

Registered in England & Wales Company No. 07601085