MOBILITY: "THE THREATS ON THE INTERNET ARE SUCH THAT WE CAN NO LONGER TAKE SHORTCUTS"

Mobile solutions have been revolutionising the business landscape for a number of years with the growth of connectivity and coverage in the civilian and commercial domain.

The energy sector has been slightly behind the curve in terms of adaption and adoption of mobile device technology to fit its needs.

In the following interview, we speak with an enterprise architect at the biggest UK energy supplier about one of their leading mobility projects and the structural and cultural obstacles to implementation.

SPEAKER KEY

TH **Tim Haïdar**, Editor In Chief, **Oil & Gas IQ**
JL **Chris Patten**, Enterprise Architect, **British Gas**

TH Chris, thank you so much for joining us today. You have been working on a very interesting project at British Gas, could you give us a taster of what it has entailed?

CP Hello, Tim. Very nice to be speaking with you. The project that you are referring to and my role within it is leading a platform initiative to provide a secure platform for sharing various services and application program interfaces (APIs) with third parties and mobile devices, particularly focusing on field management.

TH Chris, what have the key challenges been in this initiative?

CP So, one of the key challenges is managing the expectations of both our business sponsors who are wanting to accelerate the sharing of information and info sec, and regulatory teams who are wanting to make sure that things are done in a secure manner that conforms to our regulatory requirements.

These two forces actually push in opposite directions and one of the challenges for anybody putting together a platform initiative to share data through APIs is that neither of those forces can be resisted. They both need to be taken on-board and a platform has to be put in place and services and responsibilities that take seriously both the need to grow services and APIs in a rapid manner to keep up with the demand of the market.

The journey that we've been through is really to learn that we need to partner with our information security colleagues and devote as much passion into that facet of the initiative and that's taken a while to do. And I would say that, broadly speaking, we've spent as much time doing that as we have actually sharing the services through APIs.

TH What would you say have been some of the lessons learned whilst you have been engaged in this process?

Some of the lessons that I've learnt over the past year are that the info security as a topic has mushroomed since I last engaged with it a number of years ago. And one of the big challenges for any project or platform initiative within organisations is really just the sheer scale of the topics that need to be covered. So, a common risk is that people will underestimate the effort that's involved to make such a platform secure. That's the first lesson that I think is worth focusing on.

The second thing is that there's a certain approach that would seem to work with info sec, and that is that a really a systematic approach has to be followed. We need to have an approach that assumes everything the info sec and compliance officers require, is required and to aim for 100 per cent compliance.

Whilst at the same time realising that that may be quite challenging, it allows us to actually build a partnership with them so we can be seen as trusted collaborators, people who take their topic seriously. And then when the trust is built the relationships improve and we get to a point where we have some type of shared endeavour where the info sec organisation benefits from the fact that they have a platform for a known security posture rather than having to chase lots of different initiatives that are all trying to solve security issues in a piecemeal fashion. So we're talking about simple economy of scale really.

Now, add into the mix that senior stakeholders often have demands that need to be immediately met, and there is the tendency to cut corners in our industry. I think that the current state of the internet and the threats on the internet are such that we can no longer take shortcuts.

Much of the work we have done to secure the platform is fairly humdrum and rudimentary but it's work that is very frequently missed off.

So it's really just the commitment to really finish things, do them properly, to welcome the info sec guys and the compliance people into the initiative and work together to build a platform that's as secure as it needs to be to allow these services to be protected when they're exposed outside of the organisation.

TH You brought up two things in particular, in the course of your answer: trust and becoming a trusted partner, and welcoming these info sec and compliance people into the team, so that is culture and culture change.

What is going to drive trust and the culture change in order for that to be a standard part of working process?

CP That's a good question. I think the trust and the culture change necessary to gain that trust is really based on the fact that info sec is a very specialist domain, whereas software delivery is maybe a bit more generalist.

I would argue that it's actually easier for a more generalist community to move closer to the more specialist than the other way round.

I think it's important that developers and other people working in networking and databases and these other elements of the ecosystem in IT project delivery need to become more informed about info sec, because it's easier for them as resources to get clued up rather than vice versa.

So, I think really that trust is about the delivery teams becoming more literate in these many topics that are associated with information security, you know. And indeed a lot of the members of the team have started a fairly general knowledge of IF security and are now able to converse in a far more detailed conversation with our info sec colleagues because they've learnt a lot of these disciplines to the level necessary to engage properly.

I think the more flexible party has to bridge that gap and in our case it's the development team; I think that probably would be true for a lot of people.

TH One of the things that is naturally going to happen in an oil price downturn cycle is a lot of capabilities being be farmed out and outsourced.

It is seen as easier to cut training and slash softer skills budgets. How do you see that playing out for mobility in the oil and gas sector?

CP That's another good question. One of the challenges with outsourcing is that, while there are many benefits there are also some things that need to be really understood.

Modern technology often allows a small number of people to achieve some pretty big things. A lot of modern technology around automation and cloud is actually about driving costs down through improving the productivity of skilled workers.

Sometimes outsourcing arrangements can be driving the cost down by driving the cost to resources down through, moving IT functions offshore.

There is a definite tension between these two approaches and I think outsourcing could lead to information being lost from the organisation.

I think that a company even it has outsourcing arrangements still needs to be able to patrol its borders. So, I would argue that there are some functions that should probably be judiciously retained.

The danger is that while paper money was saved, risk may be pushed onto project budgets.

TH Chris, thank you so much for your time today.

CP My pleasure, Tim.

OIL & GAS mobility Calgary
KEY TOPICS AND DISCUSSION POINTS TO BE HIGHLIGHTED:
ENHANCE YOUR LEARNING EXPERIENCE BY ATTENDING: