The Digital Transformation of Public Services will fail unless Cyber Security is at its core

JC Gaillard
Managing Director
Corix Partners

Corix Partners is a Boutique Management Consultancy Firm focused on assisting CIOs and other C-level executives in resolving Cyber Security Strategy, Organisation & Governance challenges.

In July 2015, Corix Partners co-sponsored an Open Forum event in London around the theme "Digital Public Services: Rethinking, reshaping and rewiring services". For us, having worked all of our lives for and within the private sector, it was a discovery exercise – aimed at getting an understanding of some of the dynamics within the public sector, essentially around our niche consulting area which is focused on Cyber Security Strategy, Organisation & Governance.

From our perspective, any definition of "digital public service" was always going to have the Internet as its engine – together with the vast proportion of citizens connected to it through a growing variety of devices. The Internet cannot be seen as a neutral media. It is a hostile environment where countless virulent threats are active – and there can be no digital public service of any kind without a strong cyber security. So we were expecting cyber security to have a degree of prominence in the debates.

The fact that cyber security was hardly mentioned at all by any of the speakers on the day was a very concerning factor for us and it seems to conflict heavily with the message central government is driving. It left us asking ourselves where cyber security genuinely fits in the agenda and in the mindsets of public sector IT leaders.

Since then, we have observed similar attitudes very often, online, on social media and elsewhere.

For example, the 2015 SOCITM annual conference, the leading public sector ICT event in the UK, did not have any session dedicated directly to cyber security across its 2 days, and its 2016 edition is apparently planning to dedicate only 15 minutes to the topic (pending confirmation of the content of some keynote speeches and breakout sessions).

This is very hard to reconcile with the message coming from government leaders: Because of the sensitivity of what it does and its level of threats exposure, the public sector must lead the way at all levels on cyber security.

Cyber security cannot be taken for granted. It should not be seen as a low level technical problem, or another layer of technical "nuts and bolts" required to tick boxes mandated from above. It cannot be treated like something of extreme complexity that has to be left to the intelligence community, or seen a "necessary evil" that is at odds with functionality.

Cyber security must be at the heart of the public sector IT agenda and must be seen as a necessary barrier against real and active threats. It needs to be actively implemented at people, process and technology levels. It needs to be embedded in the mindset of all parts of the public sector for digitalisation to work.

Otherwise, cyber threats can and will derail the digital agenda. The citizens' trust in digital public services would be badly damaged by the type of aggressive media coverage that surrounded the TalkTalk data breach in October 2015, and this may be irrecoverable.

Change in that space is very highly vulnerable to ambiguity: It starts with a clear vision coming from the top that must be relayed without fail at all levels. All actors in the public sector digital transformation sphere must place cyber security at the heart of each and every public communication they make. Those who think it might "scare people" are just in denial about the reality of the threats and the impact they can have. It is only at this price that the digital transformation will be successful at the pace the Government is marking.