Embracing disruption to manage risk

CORE ISSUES

- The Digital Transformation journey
- Quantifying risk
- How to mitigate risk
- The role of the cloud

THE DIGITAL TRANSFORMATION JOURNEY

Organizations found themselves at different stages in the digital transformation journey. One company was just starting a move into the cloud, using a mix of public and private environments, while others were more advanced, and one was cloud-based from the outset.

Generally, there was a desire to hasten the journey but legacy infrastructure and risk act as brakes on progress, so the speed of disruption varies but is increasing. While one company said it was able to move at its own pace, a software company found that at one point customers changed their behaviour so quickly that within a couple of years, the organization needed to conduct a massive effort to re-architect all its products for new platforms.

Another company found the prospect of digital transformation 'scary' at first but found that a risk assessment brought matters into perspective, with a transparent approach to the process being key to achieving buy-in.

QUANTIFYING RISK

Security is still perceived as a risk on the digital transformation journey, although the digital economy is driving change in appetites for risk. Consequently, there is strong support for the view that risk can be outsourced, so that the service provider shoulders most of it, although there is recognition that the buck ultimately stops with the CIO.

There was agreement that certification plays a big role in risk mitigation by ensuring – by inspection if necessary – that a partner is qualified to deliver high quality levels of security, processes and management. The risk of non-compliance remains a key issue for financial services and other highly regulated industries and here, as in other areas, certification of service partners plays a big role. For others, it means ensuring that geographically sensitive data remains local, and in one case, that no foreign organizations could access that data.

The risks associated with shadow IT also need to be mitigated, again with support from top management, although this view was tempered by the recognition that many top managers are users of unofficial IT services – the security team needs to highlight the riskiness of such behaviour. Risk awareness needs to be higher throughout the organization.

KEY TAKE-AWAYS

- Cloud computing services and technologies are key to digital transformation
- Trust in infrastructure and service provider partners is key to reducing risk
- Disruption will happen anyway, so risks need to be managed
- The role of IT in the organization is undergoing massive change.

The view was expressed that disruption is essential, as the risk of not undertaking a digital transformation is that the competition may act first, although if this occurs, at least there may be lessons to be gleaned from the first mover.

HOW TO MITIGATE RISK

Risk mitigation measures are key, starting with the acceptance of risk as a fact. For example, IT equipment, - hardware and software - does fail, so risk mitigation means planning for the event. This in turn means risk acceptance needs to go to the top of the decision-making tree, not least because it is common practice for potential customers to conduct inspections as part of their due diligence. At the same time, the security or IT organization needs to be seen as a business enabler, not as the group that likes to say "No."

A discussion around risk mitigation saw disaster recovery in its broadest sense as a key solution, including using more than one cloud provider, while accepting that cloud's attributes include management overhead as well as elasticity, flexibility and lower cost.

Traditional risk management measures such as firewalls and SLAs remain useful but in limited circumstances.

THE ROLE OF THE CLOUD

While moving to the cloud is seen as an essential element of digital transformation, it is clear that the journey is not simple. Cloud's benefits of speed of provisioning, flexibility and cost are all clearly recognized but legacy infrastructure and services remain and need to be amortised and/or integrated. One less-recognized benefit of the cloud is the ability to learn from the provider about best practices from others in the same and other verticals. Cloud services brokers may have a role to play here.

Cloud adoption will change the role of IT from keeping the lights on – 'server-hugging' as one participant put it – to a focus on the business, entailing a change in IT's internal business model. In future, IT staff need strong collaborative skills, and the ability to work with partners to build a strong relationship and a commitment to openness. While the transformative journey's outcome may require fewer staff, one company supported the re-training of surplus IT staff, following which all found jobs with cloud service providers.

One participant pointed out that before the advent of cloud, the flashing green and amber lights on servers were a physical proof for IT managers of things going right or wrong respectively. In the brave new world of cloud, in the absence of direct physical proof, Cloud Service Providers must be able to assure their clients that there are no amber lights. It is a question of visibility and trust between the service provider and the client.

CONCLUSIONS

- Digital disruption is essential, not optional
- Speed is now more important than risk mitigation
- The need for risk mitigation needs buy-in from the top
- The development of a trust relationship with partners is key to risk mitigation.

"Cloud adoption will change the role of IT from keeping the lights on – 'server-hugging' as one participant put it – to a focus on the business, entailing a change in IT's internal business model."