Six steps to the next generation IT estate

The challenges facing businesses and their IT Infrastructures

By Jason Hill | Published: 12:52 GMT, 10 March 11 | CIO UK

If CIOs are not seeking to take advantage of the opportunities afforded by cloud computing they could be placing their organisation at a competitive disadvantage.

The challenge facing CIOs is to be green, secure and to deliver a 'next generation IT Estate' that will allow the organisation to provide users with access to increasing number of connected devices.

Users and customers are demanding an IT experience that is: Anytime, Anywhere, Always on and available via mobile, tablet, TV and the PC. The cost of provisioning an almost infinite number of devices to the 'network' coupled with the potential cost of security breaches is on the mind of the CFO and CEO. Running the next generation IT estate could drive costs through the roof and it may prove impossible for traditional IT operations. Even if the IT department could connect and configure this huge volume of devices, how can security be maintained with so many connected nodes?

There are currently eight billion mobile devices globally and the number is growing daily. This will be dwarfed by the number of intelligent devices in cars, white goods and even clothing in the near future. Industry is pushing forward with contactless pay, proximity awareness, gesture recognition and mobile commerce in order to capture market share.

The CIO challenge is not simply having devices that run on the 'network' but devices that self register, self configure and self secure in line with IT infrastructure and ICT policy. Devices will need to run human driven transactions but also communicate with other devices and data collectors without any human interaction or contact. This will be a huge shift for the provision and consumption of information, but also for the delivery and support of IT services and operations.

Decentralised Security

Think of traditional IT security models as akin to moats around castles; users are either inside or outside. This was adequate when few external connections were required and where all devices were also physically inside. However, as described above, the Internet of Things line of thinking means that the number of external users, devices and connections is increasing and will continue to increase. Traditional IT security delivers a hardened perimeter that is at odds with the way business and business models are operating and changing.

In a decentralised security model, each device and its data will be intelligently provisioned and secured through automated, non-human procedures. Information context will not be assumed and information security will be provided at the appropriate levels using techniques such as anonymity, cryptography, access and authorisation.

What can be done?

As with most technological challenges, software vendors, hardware vendors and consultancies tackle a point problem with a specific context. A quick internet search can turn up pages relating to green, cloud or security but few if any look at the potential dichotomy between these trends. More so now than ever is a holistic approach to delivering the next generation IT estate an absolute necessity.

Thankfully, tackling the problem space for the next generation IT estate is not insurmountable and below are some simple steps to put CIOs on the right path:

1: Extended Enterprise, the Rich Picture:

Visualisation of the future is a key enabler to success. It is possible to build a rich picture for the business of tomorrow depicting both the upstream and downstream entities and operations, and how the IT interactions underpin the organisation's capabilities. This picture becomes a powerful communication tool to central discussions and debate for investments, and envisioning threats and opportunities. It can also help in positioning the current trends to hone in on potential areas of impact.

2: Tomorrows Business, Today:

Look at the business and the business goals and consider where the competitive advantage can be gained. Group the business goals as Planning Themes that represent potential differentiation and investment opportunity.

One can identify the business and IT capabilities that are needed to support the planning themes and group them in to planning scenarios. A planning scenario will represent the likely combination of capabilities across business units or business events. This can be matched against the current programme portfolio and assessment can be made of what internal programmes that may be affected. With the current and future capabilities understood, the business context can be a passed to strategy and architecture planning.

3: Strategy and Architecture Planning:

The geography, resources, assets, and constraints of the business must be considered as a whole. There should be one view of the Enterprise Architecture that is owned by the business (where the business and IT are one in the same and aligned through the architecture). The current and future states are defined with a clear roadmap and investment plan to support the programme portfolio. The dependencies for the next generation IT estate can be clearly identified and projects can be coordinated to deliver in an optimal way.

4: Threat Modelling and Security:

Where, when, how and by whom business is transacted and information exchanged can have a profound impact on cost and brand value. With a clear view of the requisite business operations and capabilities and; armed with the knowledge of what will be Mobile or Cloud enabled it is possible to model the associated threats and risks. A measured assessment of the threat or threats that exposing information within or without the 'Extended Enterprise' will have is used to inform decisions based upon the potential impact of a breech in contrast with the expected cost of security.

The security context of devices and information within and without the control of the business should be considered with all IT projects and systems changes. Security for the Internet of Things must be designed and delivered by default. Only with conscious decisions and true impact assessment should security be removed.

5: Business Change for IT Delivery:

The culture and the way users interact with technology, the way businesses and business partners provide and consume information in a secure manner is and will continue to change. The demarcation of personnel devices versus business devices and corporate versus consumer devices is blurring beyond recognition. The Internet of Things, green IT, decentralised security and cloud computing are so fundamental in nature and so inextricably linked to the business model, operation and performance that a business change approach must be taken. The implications, benefits and risk of change must be considered in the definition and delivery of IT and business products.

6: Secure Augmentation and Implementation:

With the Internet of Things and device independence it will not be possible for IT departments to procure, provision and operate the requisite number of devices required for future business. The use and adherence to open standards for policy and protocol are a must. Developers must be aware of and account for the context and content capacity of different user and machine devices. Devices must be able to connect and assimilate to the 'Enterprise Network' with the appropriate security and dynamic policy management.

IT Projects will deliver services that use current IT implementation techniques as well as new practices that augment hardware and devices that are owed by the business, business partner, customer and consumer.

The Next Generation IT Estate is happening now and its proliferation will continue to gather pace. Unless the needs for the Next Generation IT estate are addressed holistically and within the context of the 'Future Business' there is a real and present danger that the cost of provisioning, running and securing a IT Infrastructure will not only become an impossibility but will also have a disastrous effect on business.

The tools, techniques and practices required to capture the immense business opportunity whilst safeguarding costs and managing risk are available today: albeit targeted at point problem areas. By taking a holistic business led approach, moving today's data centric IT infrastructures to the Next Generation IT Estate need not be painful and need not cost the earth.

About the author:

Jason Hill is managing director at independent IT consultancy, Glue Reply. www.gluereply.eu