simplisys
SERVICE DESK

How will ‘The Internet of Things’ impact your IT strategy?

Introduction

The Internet of Things: Do I need to worry?

You will have heard a lot about the 'Internet of Things' (IoT) recently, where people are predicting that everything from your toaster at home to your coffee maker in the office will be connected.

The question that seldom gets asked, and even less often answered is what does that mean for the business world? How will it impact my job and the company I work for?

The reason that answers are so few and far between is that this is shaping up to be an archetypal disruptive technology. It will change not only how we work, but how we think about the work we do in ways that we can't yet imagine and certainly can't predict. It's not just about 'smart' devices but smart sensors, smart tools and even smart office furniture. Imagine an office chair that monitors your posture and alerts HR that you may need to have a workstation DSE assessment automatically!

So, what can we predict about the challenges the Internet of Things will present us?

Surprisingly we can already anticipate quite a few areas where this new technology will impact both our working and private lives. These seem to fall into two general categories, the technological challenges and the process / operational.

Technological Challenges

One of the key aspects of IoT is the fact that they are connected. By this we usually mean connected to the internet but actually it is most likely that most uses will limit the connectivity to our internal networks. This connectivity raises a number of questions:

Security: How will we secure these devices? Manufactures of commodity devices, which will undoubtedly comprise the bulk of the IoT do not have a great track record of making them secure.

Consideration will need to be given to securing them at a network level. Implementing VLan separation will become standard, possibly not just putting IoT devices on a separate VLan but potentially individual separate VLans for different types of IoT devices as well as separating them from 'normal' network traffic. Obviously implementing firewalls between these diverse VLans will present both a management and design challenge.

Network Connectivity: It is unlikely that these IoT devices will come equipped with a cat 5 / 6 network socket. So how will they connect to the wider network? Most likely via WiFi, which raises the question of managing WiFi bandwidth usage and network congestion? Each WiFi access point is after all a single collision domain. It will become important to ensure that the IoT devices have adequate connectivity without compromising the ability of users to access the WiFi infrastructure.

It is possible other technologies may well come to the fore, such as Ethernet over Power or Near Field Communications (NFC) or Bluetooth. In either case consideration on both the connectivity architecture and any 'back haul' requirements needs to be built into our current plans so as to be ready for the future.

Protocol Proliferation: Will IoT devices talk 'TCP/IP' and if so, does your addressing space allow for the vast increase in connected devices? Will they use a common protocol such as http in their communications or some other as yet to be defined and agreed protocol? If it isn't a "well known" protocol will your routers and firewalls handle it correctly? Will it integrate with your existing network monitoring tools? Is it time to consider looking at Software Defined networking to attempt to futureproof your infrastructure?

Operational Challenges

As discussed the IoT will probably bring many changes to the way we work and the way we do business and like any disruptive technology it is impossible to predict with any accuracy what those changes will be and what impact they will have. Just as with the technological challenges we can, I think, predict some of the operational challenges that lie ahead.

Management: The sheer number and variety of the IoT devices

that we will be using will make management challenging, both from a setup and configuration point of view and also asset management exercise. Do current Asset Management tools have the flexibility to record information about these devices that we simply may not have thought of, how do you provide a field to record something when you have no idea of what that bit of information might be? Its format or meaning? Can IoT devices be configured and managed remotely using your existing tools? What if they need obscure command line / PowerShell scripts to be run to manage them?

Information Volume: One of the key aspects we can see coming out of this revolution is the massive increase in information available to users, support staff and management. It is predicted there will be a plethora of IoT devices reporting status, management and possibly monitoring information. Does this data need to be stored? If so, where will the data be stored? How easily will you be able to access the data and create meaningful reports?

Privacy: As we suggested the office chairs may well be reporting back to HR on the posture of the person using it. This information would definitely fall into the category of private and subject to the provisions Data Protection Act. Disclosing the fact that a person may have a medical condition, for example a bad back, is a sure-fire way to attract the attention of the Legal Department!

Ensuring that access is restricted to this sort of data, maybe requiring the use of encryption, may mean either having to specify IoT devices that support such technologies or having to implement it at the network layer.

Conclusion

While we can't tell what the IoT will bring in the way of change to our working and personal lives, one thing is sure. This disruptive technology will change the way we work and even think about work. It will impact our businesses in ways we can't imagine and require changes in our working practices and processes that most current tools simply cannot cater for. If there is one take away from this, it is that we need to be thinking about IoT now, not when the new technology hits. We need to be prepared for whatever it brings and to that end whenever we are thinking about purchasing tools,

implementing processes or devising strategies at the core of our considerations should be the need to build in flexibility. A flexible response to the changes that the IoT will bring is going to be the best, and only, preparation we can undertake.

Simplisys Ltd the specialist in Service Management.

Simplisys Service Desk is designed, developed and supported by a team of dedicated staff at Simplisys Ltd based in Bristol, England. Simplisys Ltd is an ISO 9001 registered company and delivers solutions to industry best practice and quality standards. Steve Payton said "Our design philosophy is to maintain leadership in our space by monitoring new and emerging technologies and creating software development roadmap that future proofs our products today and in the future".

For more information go to:
http://www.simplisys.co.uk/solutions/enterprise-service-desk/

.

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk