It's time to embrace (and prepare for) the shift to the Cloud

The software industry is entering another age of astonishing innovation. It's a time when not only is software advancing at an astounding rate, but so are hardware devices – where power is increasing as quickly as size is decreasing, and software and computing power is becoming near ubiquitous.

Consider this: a handful of years ago, few would have believed that customer relationship management software would have moved almost completely to the cloud. Or that Lotus Notes, that grey old lady of IT, would have made the jump as well. Even among the proponents of Cloud Computing, few believed corporate software and data wanted to be liberated so quickly – and make itself readily available anywhere, anytime, on any device, and from within any Web browser.

No doubt, along with all of the benefits of SaaS will come new risks and challenges. This is especially true as even more mobile devices access critical corporate data. Consider the fact that one out of ten laptops in use today will be lost or stolen, and you know most will not be encrypted. Then, there's the challenge associated with securing new Cloud Computing architectures, and all of their various shapes and sizes. I'm sure that in the years ahead, there will be a number of negative stories surrounding Cloud Computing. Providers will go out of business. There will be a number of system outages that affect large numbers of customers. And there will be a number of data breaches.

The IT Challenges facing organisations

Yet, I believe that the SaaS and Cloud Computing revolution holds the potential to benefit everyone in the software industry, and all who rely on it for their business. For instance, we in the industry are well aware that software is evolving too quickly to keep up. It's a never ending process of software enhancements, upgrades, security fixes, and new installations. And, few would disagree that there are too many vulnerabilities affecting too many applications. In this disorder, most of the burden has fallen on the shoulders of organisations that have had to dedicate extraordinary resources to patch and mitigate the security holes.

Here is an interesting statistic that reveals the magnitude of the challenge. According to Qualys' The Laws of Vulnerabilities 2.0 research, companies take an average of 59 days to patch their vulnerabilities. Five years ago, that number was 60 days. That's a reduction of one day in the past five years. When one considers all the effort and automation that has gone into patch management in the past five years, that's not much in the way of improvement. And this shows not just how steep the challenge is, but just how broken the current ecosystem of traditional software is.

The SaaS approach

Fortunately, the SaaS and Cloud Computing models are positive disruptions on the infrastructure of both private networks and the Internet. Unlike when individual organisations patch (work that must be duplicated for every installation), when SaaS vendors update their software applications, all of their customers are patched instantaneously as well. Because of this simple fact, many of the security problems that plague today's business-technology systems – such as patches and software misconfiguration issues – are solved. Thus, in this, and many other ways, the burden of maintaining a secure application largely is transferred from the software user to the provider. The effect of proper patching is amplified throughout all the IT systems the SaaS and cloud providers touch.

For many years it was thought that SaaS would be destined just for SMEs, but today we know that this isn't so; the advantages of cost reductions in staff and

The author
Philippe Courtot, CEO of Qualys

infrastructure are as valuable to the large corporate as the small or mid-sized business, particularly in the current economic climate. Cloud Computing offers a delivery model that scales and can reach out to millions – that's the power of the Internet. Once the infrastructure or data centre has been built the cost of adding additional services is minimal and hence the service provider can offer aggressive prices because the overall cost of the infrastructure and the specialist personnel to man it can be amortised over a large number of users.

Another massive advantage for customers of SaaS is that it puts the power in the hands of the buyer. They can 'try and buy' solutions with ease and of course they are at liberty to switch vendors if their services don't come up to scratch. What's more whilst vendors have traditionally focused on the enterprise as the customer for hardware and software, the data centre owners will gradually become key customers for the future. For the industry overall cloud-based computing will mean a massive change and it will be those who adapt and change with the market who will be the winners of tomorrow. As with any major industry evolution, there will be consolidation amongst existing players and some new entrants. Who would have suspected five years ago that Amazon.com would be one of the new players in the market, but with change comes new opportunities and new challenges for us all.

Why, you may ask if the future of cloud-based computing is so rosy hasn't it happened sooner? It has taken over ten years for the revolution to slowly happen. Some of this has to do with the natural pace of change of such a fundamental nature for the industry. Other issues that slowed progress include the limitations of Internet availability. Also the bursting of the Internet bubble back in 2001 when the early innovators, like Qualys, were in the early stages of development of their infrastructure and this halted the momentum, as VC investment disappeared and SaaS entrepreneurs were forced to find alternative modes to fund their growth. In 2005 when the VCs returned the market regained its momentum and today as a result we are seeing a tsunami of new SaaS applications appearing on the market.

Resistance is Futile

Some still are fighting the shift to SaaS and Cloud Computing. But, I don't believe that resistance to the transformation of on-premise business IT to cloud-based computing is a viable option. Not for long. The business benefits, cost savings, and reduction in complexity are just too compelling for businesses to overlook. Actually, today, the strongest resistance we see is emanating from IT departments, and IT security staff – mainly out of fear of what might happen if one were to lose control of data. But the reality is that businesses have already lost control of data, as evidenced by the constant security breaches that we read about in the media on an almost daily basis. By putting the data in one place it is easier to control access to it. Security in the cloud will follow the pattern of banking where we are comfortable to withdraw our cash from the convenience of an ATM, over the Internet or via our mobile and leave its security to be dealt with by the experts.

Nevertheless, despite reservations from IT, businesses will march forward, because the business has no choice but the path that simplifies many of today's IT complexities. And in this, the primary – and strategic – role of IT security will be successfully and securely managing the privacy and security risks associated with data living in the cloud.

The Missing Pieces

While the SaaS and Cloud Computing revolution is well underway, there still is much work to be achieved before the core infrastructure and associated services are as secure, reliable, and trustworthy as they can be. For instance, we need ISPs to coordinate so that network traffic flows more cleanly, and is free of malicious packets. We'll also need a simple, globally recognised way to recognise and manage the identities of people and devices and a more secure browser. Other key aspects that require attention include developing a legal and contractual framework that ensures compliance and provides effective SLAs.

There is also the crucial business of defining accurately how enterprises can integrate and secure their current infrastructure as more of it is moved to cloud services. Vendors must abandon their traditional proprietary approach and work together to develop standards that allow data in different clouds to be shared. For this effort, I encourage all businesses, security professionals, CIOs, and vendors to work together to make the transformation as beneficial as possible for all. Some of the organisations working hard to ensure that we build this new cloud infrastructure right from the beginning include the Cloud Security Alliance and the Jericho Forum, both of which are promoting Cloud Computing best practices.

While the visible shift to Cloud Computing to date has been the movement of applications and data to the cloud, it's not going to stop there. Soon, the day will come when companies outsource not only their software but their network infrastructure, as well. One day, almost everything we do on private networks – manage information, applications, infrastructure, and services – will be accessible instantly and securely from anywhere and from any Web browser. It's time to prepare.