

## The IT security threats and opportunities posed by 'Bring Your Own IT'

by Patrick Oliver-Graf, Director, NCP engineering

Initially SMS was perceived as a second-best option to calling. Now, with a growing array of smart devices and available media 'bites', the attraction of this social media messaging is so great that employees do not wish to part with it even at work. This started a trend of 'bring-your-own-IT' to the workplace. Employees now demand to get connected to the corporate network and applications. This 'consumerisation' may well increase productivity, but will also bring new risks to corporate data integrity and network security. Businesses must re-consider their security policies and available tools, such as VPN to mobile devices and data encryption.



*Patrick Oliver Graf has a proven track record of growing business and generating tremendous returns during more than 17 years in the marketplace of high technology and security. As International Sales Director of NCP he is responsible for expanding NCP's global business. Besides that he is General Manager at NCP, Inc. in Mountain View, CA and is responsible for NCP's North America operations.*

*Prior to NCP, Mr Graf was International Sales Director and Vice President Marketing at HOB, where he successfully built an entire global distribution and reseller channel. He has also established the North and South America operations with subsidiaries and distributors.*

Sending a note has never been easier, with people of all ages and seniority today being able to send an SMS message around the world for just a few pennies. Initially, users perceived SMS messaging as merely a tool for keeping track of their children's whereabouts and did not foresee the trend for instant, non-invasive, text-based communication that was about to unravel before them. Within the last decade or two, we have seen communication tools enhanced to a level that far exceeds any previous predictions. The result is a growing appetite for the messaging and increasing reliance on 24/7 dialogue at the finger tips.

The demand for tools that exchange interactive 'text bites' of communication is continuously growing, due to the flexibility and cost savings they offer over other traditional forms of communication, such as

the telephone. Globalisation has also had a major impact on the need for cost-effective media that enables people to interact with others around the globe, instantly and affordably, both in their personal lives and in their corporate roles.

This demand has led to the success of a number of social media sites, including the ubiquitous Facebook, Twitter and LinkedIn, which enable users to interact using 'text bites' of communication very easily, while on the move and at their own leisure. So, what impact has this had on the adoption of new communication tools and the way we use them?

Independent analyst house, Gartner, has stated that consumerisation is now the primary driver of the mobile space, and warns that CIOs must be ready to embrace

a range of more flexible approaches to their mobile strategy. The growth of smartphones is expected to rocket in 2012, with Gartner predicting sales of smartphones to reach 645 million in 2012. Gartner also states that more of these devices will find their way into enterprises as employees entering the organisation will expect to be allowed to use them. Further still, Gartner estimates that 18 billion apps will be downloaded in 2011, up 114.5 per cent from 2010 and will rise to 31 billion in 2012.

These statistics highlight a clear change in society, particularly in the way we are accessing information and communicating with one another. The consumerisation of IT is already having a huge impact on the corporate world. Employees are using their own personal mobile devices in the workplace and behaving more like

consumers. They demand a wider variety of devices and strategies, such as 'Bring Your Own IT' at work, to enable them to operate more freely and in many cases, more effectively. This trend has put a great strain on IT departments, who not only have to handle the growing demand from employees to get their personal devices connected to the corporate network, but also have to tackle the major IT security risks involved in doing so.

Allowing employees to use their personal devices to connect to the corporate network and access corporate data insecurely could be potentially damaging to a company. In 2011 alone, we saw a number of cases where corporate data had been lost, leaked or hacked. The most notable is the Sony crisis, where they had to announce that the personal details of 77 million Playstation users might have been stolen by hackers. Not only did this tarnish the company's brand, it had also a negative impact on its share price, which dropped significantly. The challenge for CIOs is therefore to ensure complete data and network security when accessing the corporate data or the corporate network using a personal mobile device.

There appears to be a grey area over whose responsibility it is to ensure that employees' personal mobile devices are fully secure when accessing the corporate network. It is also unclear whether it falls under the CIO's role to ensure that all employee personal mobile devices are connected to the network. It is in both the employees' and employer's interest to ensure that corporate data and the network integrity remain secure at all times. However, it is the CIO's role to ensure that an effective strategy is in place to manage the use of personal mobile devices at work. Those choosing to ignore the shift in work ethic may be left to face the consequences, with insecure devices jeopardising data and network security, potentially becoming the next public case where customer data has been lost or compromised.

One of the major factors affecting whether an organisation implements a good strategy is the cost involved. Many organisations will see initiatives such as 'Bring Your Own IT' to work as yet another strain on their IT budgets. With severe cuts being made across all departments, it is likely that IT security will suffer. Although many departments are vetoing the use of personal mobile devices in the workplace, they are not investigating whether they can indeed be used securely. Ensuring that all corporate data and the corporate network are fully secure is paramount to the success of an organisation that puts its customers first.

The benefits of implementing a good 'Bring Your Own Device' to work strategy

will, in effect, increase an organisation's competitiveness by improving both customer service and employee morale. The flexibility of being able to use a personal mobile device at work or remotely is a clear advantage for many companies, with employees being able to access all the information they need and respond more efficiently. Research conducted by Citrix Online revealed that companies typically saw a 30 per cent rise in employee productivity.<sup>1</sup>

The days when companies had to provide corporate smartphones, a laptop and a tablet PC (which is a rising trend today) are coming to an end - potentially freeing up thousands of pounds of a company's IT budget. To ensure that a 'Bring Your Own IT' strategy is effective, IT security needs to be at the forefront of the business' priorities and importantly, the CIO's agenda. This includes enforcing clear policies covering IT security, management and HR.

There are a number of technologies that can help to manage workplace technology. Companies should seek an IT security tool that will ensure secure operations both in and out of the office, with staff being able to access and share vital data securely across both corporate networks and external networks. A Virtual Private Network (VPN) technology does exactly this, by enabling users to access their data and corporate network via a secure connection, encrypting data at the source and delivering it safely.

All VPN tools currently on the market contain IPsec (*Internet Protocol Security*) functionalities, a protocol suite for securing Internet Protocol (IP) communications. However, there are differences in IPsec solutions, which businesses need to take in to consideration. A quality VPN tool should have an IPsec protocol-stack, which matches all the IETF objectives and supports all IPsec standards. Such tools should be easily configured and compatible with popular operating systems, including Android - enabling seamless roaming for applications that are always online. Businesses can ensure complete data security whether employees are using the corporate network or working remotely from a hotspot from a personal mobile device by implementing an IPsec VPN technology that supports all peripheral and central components, as well as systems in all remote access environments.

Workplace technology and the rise of 'Bring Your Own IT' to work trends will present a number of challenges and opportunities in 2012. IT security will climb up the business agenda, and although there will always be a number of companies that do not support the change, those that do will benefit from

the flexibility and cost efficiencies it brings. As further developments in technology and mobile devices arise, it is likely that trends such as 'Bring Your Own IT' to work will become even more integral to the wider business strategy, and the importance of IT security - including preventing data loss and leakage - will become an issue acknowledged not only by CIOs, but employees at all levels. ●



**Connect-World now on  
Facebook & Twitter**

*Connect-World*, the world's foremost discussion forum for leaders in the ICT industry, is now available on Facebook and Twitter.

The world's top ICT decision makers express their opinions in *Connect-World*. They use clear, non-technical, English to discuss how ICT helps shape regional and global development. The articles essentially examine the influence that ICT products and services have on the way people live and do business. With separate editions for each of the world's regions, the reports highlight the most important ICT trends and issues influencing socio-economic growth.

*Connect-World* is now available to follow on Twitter (<http://twitter.com/#!/ConnectWorldICT>) and Facebook <http://www.facebook.com/connectworld.ict>

Also, it is still possible, for FREE, to directly access all past and present *Connect-World* articles, ICT Industry press releases, eLetters, ICT News and more at [www.connect-world.com](http://www.connect-world.com).

<sup>1</sup> <http://www.personneltoday.com/articles/2011/07/29/57835/what-is-it-consumerisation-and-why-does-it-matter-to-employers.html>