

The Consumerisation of Corporate IT

An Ethical Hacker's View

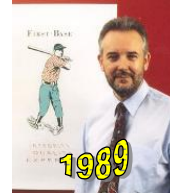


Peter Wood
Chief Executive Officer
First • Base Technologies LLP



Who am I ?

- Worked in computers & electronics since 1969
- Founded First • Base Technologies in 1989
(one of the first ethical hacking firms)
- Primary roles:
 - Network penetration tester
 - Social engineer
 - Conference speaker
 - TV and radio security 'expert'
 - Security author
 - Active member of BCS, IISP and ISACA





This Presentation



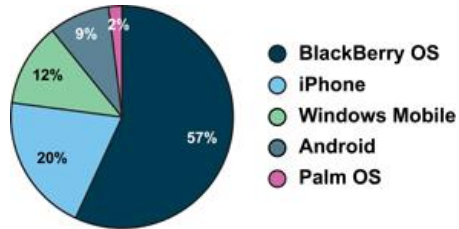
Slide 3

© First Base Technologies 2010

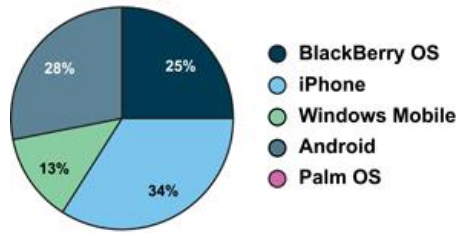
- Consumerisation: cool technologies show up for the consumer market before they're available to the business market.
- Every corporation is under pressure from its employees to allow them to use these new technologies at work, and that pressure is only getting stronger.
- Younger employees simply aren't going to stand for using last year's stuff, and they're not going to carry around a second laptop. They're either going to figure out ways around the corporate security rules, or they're going to take another job with a more trendy company.
- Either way, senior management is going to tell security to get out of the way. It might even be the CEO, who wants to get to the company's databases from his brand new iPad, driving the change.
- It's going to be harder and harder to say no.



MIT's Technology Review



Currently



In 2 Years



Booz & Co. Report



The frontiers of innovation in information technology are moving from corporate IT to consumer IT. With that shift, corporate IT is rapidly becoming “consumerized”: Employees expect to be able to use all the innovative new devices at their disposal, both to do their jobs and to maintain their always-connected lifestyles, while being able to work whenever and wherever they need to.



<http://www.booz.com/media/uploads/FriendlyTakeoverVPFINAL.pdf>



Corporate vs. Consumer IT

CORPORATE SPACE

Devices with functionality limited to phone calls and e-mail, typically BlackBerry

Restricted storage for files and e-mail

Static employee directories and cumbersome proprietary collaboration platforms

Outdated static content within corporate intranet—centralized maintenance and control

Long replacement cycles—up to four years for hardware and eight years for software

Highly standardized, inflexible, and often restricted environment ("beige box")

Mobile Phones

Storage

Innovative Services

Dynamic Content Creation

Update Cycles

Style and Customization

CONSUMER SPACE

Smart phones offering tens of thousands of useful apps, typically iPhone or Goggle Phone

Providers such as Google and Yahoo offering virtually unlimited storage

Social networks such as Facebook and LinkedIn used for both socializing and working

Blogging, wiki, social networking, and content services allowing consumers to create, customize, and manage the content they want

Very rapid updated hardware—immediate download of new apps and services

High variety of consumer devices systems, applications, and "skins"

Source: Booz & Company analysis

<http://www.booz.com/media/uploads/FriendlyTakeoverVPFINAL.pdf>

Slide 7

© First Base Technologies 2010



Booz & Co. Report



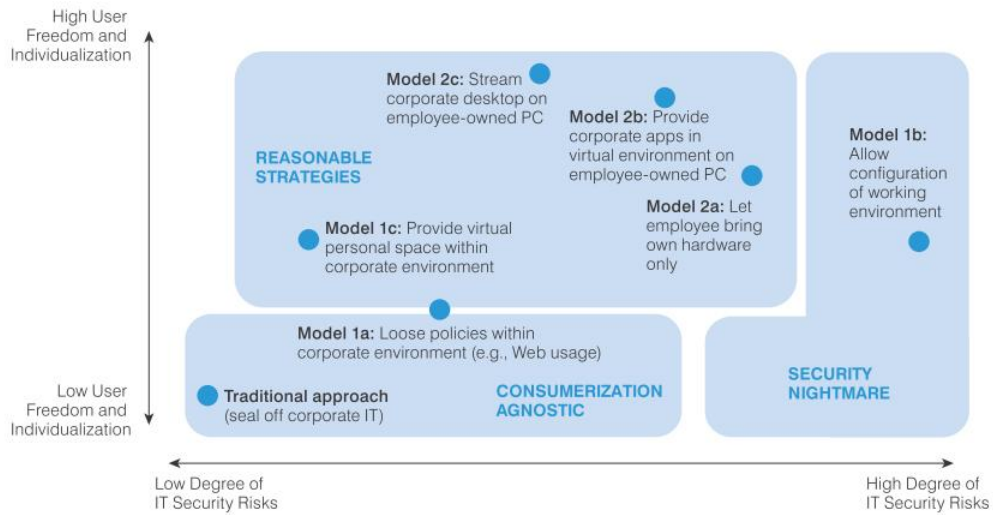
In short, the efforts of corporate IT departments to maintain perimeter security by exerting tight control over their networks is ultimately doomed to failure. Instead, CIOs must get ahead of the consumerization curve by coming to terms with what is valuable and productive about the influence of consumer IT on corporations and then devising strategies to make it work.



<http://www.booz.com/media/uploads/FriendlyTakeoverVPFINAL.pdf>



Consumerisation Models





Citrix

Citrix Australia embarked on a pilot program to test the virtues of employee-owned computers. The test involved 300 employees, each of whom was given a stipend of \$2,100 to buy a computer and pay for the mandatory three-year service agreement; half chose PCs, half chose Macintoshes.

Access to the working environment was provided by a virtual private network, with applications delivered by Citrix's own XenApps system.

The results were impressive: With the manufacturers providing support, costs to maintain the computers were minimal. The attrition rate of the computers declined, since they were owned by the users. And the employees proved more productive than their peers.

The program was then opened up to 10 percent of the company's employees - and twice that number asked to be included.

<http://www.booz.com/media/uploads/FriendlyTakeoverVPFINAL.pdf>



Intel



Intel IT is actively integrating employee-owned hand-held devices into our enterprise environment. We have long recognized that the consumerization of IT - employees using their personal devices to access corporate data - is not a passing a workplace trend, so we worked closely with Intel's Legal, Information Security, and Human Resources (HR) groups to enable a solution that aligns with our information security policy. ”

<http://download.intel.com/it/pdf/Maintaining-Info-Security-while-Allowing-Personal-Hand-Held-Devices-in-Enterprise.pdf>

Slide 11

© First Base Technologies 2010

- In January 2010, we implemented a new program allowing employees to use their own hand-held devices on the job. Employee response was overwhelmingly positive, with more than 3,000 employees signing up in the first month.
- As of September 2010, our computing environment included more than 20,000 hand-helds, and about 6,500 of these are employee-owned with access to corporate information.
- In July, we started a new program that allows personally owned tablets; we do not yet allow personally owned PCs, but are investigating that possibility for contract employees.
- Ten years ago, Intel employees came to work to use great technology. Now, with the battery of consumer devices available, they often have better PCs and printers at home than they do at work.
- User expectations have also changed: We no longer need to provide basic computer and software training—users already have experience, often using platforms that we don't have—and the Internet has become accessible from more places than ever before.
- It is relatively easy to verify and enforce which applications are running on corporate-owned hand-held devices. With personal devices, this process is not so straightforward because employees have the right to install any applications they choose. However, we have identified certain minimum security specifications for hand-held devices that provide a level of information security that allows us to test, control, update, disconnect, remote wipe, and enforce policy:
 - Two-factor authentication required to push e-mail
 - Secure storage using encryption
 - Security policy setting and restrictions
 - Secure information transmittal to and from Intel
 - Remote wipe capability
 - Some firewall and Intrusion Detection System (IDS) capabilities on the server side of the connection
 - Patch management and enforcement software for security rules
 - The ability to check for viruses from the server side of the connection, although the device itself may not have anti-virus software



Western Union

Western Union had a policy of issuing and supporting only BlackBerrys for its mobile workers.

In September 2010, a new CEO, Hikmet Ersek, demanded that he be allowed to use his iPhone for work.

This coincided with a corporate strategy to offer Western Union's money-transfer service on all mobile devices.

Reluctantly, the chief information officer, John Dick, was forced to comply.

"We need to give our employees more freedom," Dick said at an industry conference in October 2010. But he also acknowledged that it would take several months for the company to fully authorize and support the iPhone and Android devices.

<http://www.technologyreview.com/business/26634/>



BYOD



When Henry Ford introduced the Model T in 1908, the speed limit in most places - provided you were outside city limits - was just 20 miles per hour (in town, it was usually just 10 mph).

That restriction seems hopelessly quaint today. You know what else will soon seem equally quaint? Your company's repressive approach towards employees' devices. ”

Gary Kovacs, senior vice president at Sybase

<http://tech.fortune.cnn.com/2010/09/01/bring-your-own-device-to-work-is-finally-here/>

- Most companies provide a limited selection of laptops and smartphones that range from bland to blander. Meanwhile, employees are champing at the bit to bring in their own stylish smartphones (the iPhone 4 and HTC Evo come to mind), cute netbooks from Asus and Acer, and, increasingly, useful tablets like Apple's iPad.
- Most companies, if they were around then, first developed their IT management policies during the mainframe or client-server era. Administrators protected those expensive assets like high priests guarding holy relics. As we moved through the PC and Internet eras, IT, inevitably, loosened up a little. But the basic 'command-and-control' framework never disappeared.
- Problem is, we are in a new era, characterized by two transformative changes. First, the consumerization of IT means that new innovations hit the consumer sphere first before entering the enterprise. A good example is the iPad, the tablet reinvented by Apple. Despite being aimed squarely at consumers, the iPad has in just a few months already won enterprise fans such as Mercedes-Benz and Wells Fargo bank.
- Second is the emergence of mobile-centric enterprises that are adopting rather than preventing these new ways of working. Kraft Foods, for instance, is letting its 97,000 employees buy their own PCs, offering them a stipend to do so. Carfax is offering its employees interest-free loans, while Citrix Systems is giving workers a whopping \$2,100 to choose their own computer.
- Other companies, including my own, are letting employees connect their personal iPhones to corporate applications, and/or footing their monthly bills for them.
- These firms, what I'll call 'unwired enterprises,' understand how 'bring your own device' policies can empower employees to be more creative, efficient and productive. And they manage the risks of 'bring your own' policies by relying on management software that enables IT to keep personal and business data 100% separate, and consequently, secure.

Reclaim your life.

Easily manage and deploy virtual desktops. Maximum security. Empowered Users. With MokaFive, you can deliver the desktop on your terms and meet users' needs.



[Learn more](#)

Blog | [Get ready.](#) [Start.](#) [Migrate.](#)

Mac or PC, your choice.

Mac or PC? On a home computer? Work on an airplane? Yes, yes, yes.



Spotlight.

The buzz on MokaFive.



AlwaysOn's Going Green Silicon Valley Top 100
MokaFive named category winner for Data Center Efficiency

Try for free.

Download now or request the VirtualBox Player beta.





Bruce Schneier



Security is always a tradeoff, and security decisions are often made for non-security reasons. In this case, the right decision is to sacrifice security for convenience and flexibility. Corporations want their employees to be able to work from anywhere, and they're going to have loosened control over the tools they allow in order to get it.



<http://www.schneier.com/blog/archives/2010/09/consumerization.html>



Smartphone Issues

- Consumer products with corporate access
- Minimal authentication
- Frequently lost or stolen
- Data often not encrypted
- Attacks:
 - Phishing
 - Malicious attachments
 - Bluetooth attacks
 - WiFi attacks
- Provides entry point to enterprise systems



Laptop Issues

- Relies on Windows authentication
- Stored credentials can be exposed
- Frequently lost or stolen
- Attacks:
 - Phishing
 - Malicious attachments
 - WiFi attacks
 - Local Windows authentication bypass
- Provides entry point to enterprise systems



Wireless Issues

Remote workers:

- SSL VPNs
- home wireless insecurity (WEP is broken)
- unprotected WiFi hotspots



Slide 18

© First Base Technologies 2010

With a vast increase in the number of people working from home or on the move, wireless networking has become pervasive.

The average home user doesn't want to know about the complexities of wireless security (WPA PSK versus WEP etc) so most home wireless networks are inadequately protected or just plain open.

The same is true of many wireless hot spots of course, if you don't have to authenticate and enter a key, then it's unlikely to be safe.



Need more information?

Peter Wood
Chief Executive Officer
First • Base Technologies LLP

peterw@firstbase.co.uk

<http://firstbase.co.uk>
<http://white-hats.co.uk>
<http://peterwood.com>

Blog: fpws.blogspot.com
Twitter: [peterwoodx](https://twitter.com/peterwoodx)

