



Every desktop in the UK public sector could hold the key to millions in savings. **By shaving just £100 off the total cost of ownership (TCO) of each IT device, over £500m per year could be saved.**<sup>1</sup> At the same time, every device comes with potential risk. How can costs be cut without sacrificing productivity?

**How many IT devices are there on your desk right now? A computer? What about a laptop? Maybe a mobile phone or PDA? The UK public sector is home to an estimated 5.5 million IT desktops**, each of which could include any number of these devices.

**And therein lies a problem: no-one can be sure precisely how many devices there are.** Their numbers have been built up over years as new equipment was introduced and slotted into legacy systems. Large-scale IT outsourcing deals are contracted on approximate, not precise desktop numbers, leaving agencies either over-paying or under-managed.

Worse still, new devices may have been introduced to the desktop only to leave older tech underused but still plugged into the network. Compatibility and compliance issues would be inevitable, requiring more people on site to address problems. Changes in government only add to the uncertainty, as people come and go, or move departments.

Anyone connecting their own devices to a public sector network only compounds the potential risks. Such devices could include software or malware downloaded from unknown sources.

How can any public sector body be certain what's in the building or connected to the network at any given time, and how secure those systems may be?

What's more, how can any public sector body be expected to keep up? Scanning the system once a month or once a quarter might be an option, but as soon as that information is gathered, it may already be out of date.

Service level agreements with third-party suppliers provide some assurance that the system is being monitored, but without an ongoing and updated audit

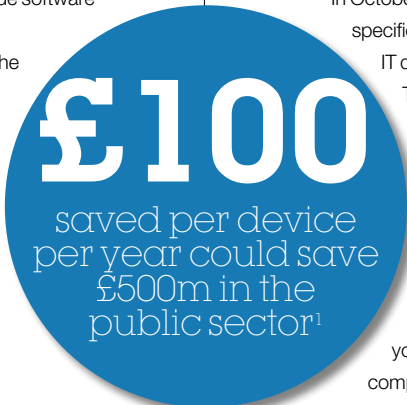
of all equipment on the system, there's only so much that can be done. Look at software asset management – how many copies of licensed software are being run on how many devices in any given public sector department? And if the organisation has bought hundreds of software licences, are they all current and actually in use? If employees have left the organisation, have their licences ever been closed? In most cases, such details are based on assumption or outdated information.

And then there is the much bigger question of cost. In May 2009, the UK government published the Operational Efficiency Programme, which claimed annual savings of £3.2bn in IT were possible – but only with major changes in ways of working.<sup>2</sup>

In October 2010, the then-government CIO and CISO John Suffolk specified that the public sector could save significant money in IT desktops, especially as "Gartner claims that best practice TCO is £1,800 a year".<sup>3</sup>

According to Suffolk, the UK benchmark in 2010 is now at £1,660, and that by saving £100 per device per year, it is estimated the whole public sector could save over £500 million a year.<sup>4</sup>

But in order to achieve all of these proposed savings, the public sector needs to start answering some key questions: What hardware and software do you have on the network? Is it all software and security compliant? What does it all cost in real terms?



**£100**  
saved per device  
per year could save  
£500m in the  
public sector<sup>1</sup>

At the moment, these are not questions that can be answered by most third-party IT desktop management suppliers. Audits are not necessarily ongoing and not all devices are covered. In addition, many organisations prefer to use the default “free” software included in any SLA with IT suppliers.

But if you’re supporting 100,000 desktops in a big public sector department, that IT supplier is likely to recommend thousands of management servers to support that software infrastructure. And that doesn’t come cheap.

What is needed is a thorough IT desktop audit, to provide the UK public sector with a clear representation of the IT assets in place, as well as determining if they are compliant and calculating the total cost of ownership in real terms, eg personnel, servers, equipment and beyond.

Once that information is in place, then the process can begin to create a more efficient and effective IT desktops in UK public sector, without overtaxing the sector as a whole.

#### PATCHES, COMPLIANCE AND ZERO DAY ATTACKS

An audit is only the start. The current government is driving efficiency and reform through the public sector. This means minimising downtime and ensuring that systems are available when needed.

Any weaknesses or faults in a system or network will need to be patched more quickly than ever, or risk bringing work to a halt.

However, while home computers may be set to download and install patches automatically, it’s a completely different scenario in the commercial world. Quite often, public sector organisations rely on their IT supplier or an outsourced systems-integrator running the desktop service to deal with patches.

And this patch management process must take into account all devices connected to the public sector workstation, not merely the PC or laptop. Servers, mobiles and point-of-sale (POS) devices all come into play. Manual patch management is not going to be enough. The risks and costs involved will be too much.<sup>5</sup>

The number of patches and updates also seems to be on the rise. For example, Microsoft released seven “critical” and three “important” updates in the months following the launch of Windows 7.<sup>6</sup> Organisations have to monitor, assess and implement hundreds of these patches and updates from a range of software sources on a rolling basis.

And while the UK public sector requires critical patches to be implemented within a set timeframe, many organisations can take months to achieve a 90-95 per cent patch success rate, according to Gartner.<sup>7</sup>

If that level of success is not achieved, it could mean some machines are not patched but are still on the network. These represent possible security vulnerabilities.

For example, zero day attacks are always going to be a possible threat so long as networks rely on a weekly patch cycle, as is the case through most of the public sector at the moment. A zero day attack takes advantage of vulnerabilities in computer applications before the software developer has a chance to patch the problem.

Patches are typically sent out on a weekly or monthly basis, but what happens if there’s something serious, such as a zero-day attack, which

takes advantage of a previously unknown vulnerability? In many cases it may have to wait until the next patch cycle, increasing that risk period of vulnerability. And patches may also need a device to be connected to the network, but a laptop may not be connected to the network regularly.

And if one PC is vulnerable to zero-day attacks, then the whole network is vulnerable. This can risk shutting down an entire operation just because something hasn’t been updated.

If you are waiting for a patch to fix one thing and that one thing is a vital part of the system, then patch management becomes an essential ingredient in business continuity, efficiency and risk mitigation concerns. Organisations must be able to respond very quickly to such a situation, assessing their exposure and then quarantining or remediating infected machines as needed.

Any IT desktop programme for the UK public sector cannot afford to be patchwork – it requires a unified approach that works across the whole network.

#### WHAT NEXT?

The UK public sector needs to clean house and find out exactly what it’s got. IBM can produce the audit needed to assess any department’s big IT desktop picture. First and foremost, it will reveal what devices are on the network and determine whether they are all compliant, not only in terms of patching, but also in terms of security and software.

The audit of software assets can be particularly useful when it comes to renegotiating the next software contract with the supplier. And from a compliance and audit perspective, it’s essential. Imagine an employee downloading a piece of software and sharing it without the company knowing. Suddenly, the company is vulnerable to charges for software licences that no-one realised had to be paid.

The UK public sector needs a system that is up to date and works in real-time. If someone downloads a piece of unlicensed software across the network, a flag should be raised. If a new device is added to the network, the system should respond accordingly. And none of this should require the kind of server power being used by the public sector at the moment.

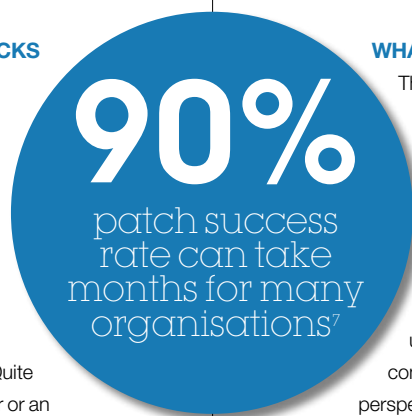
IBM’s solution can be scaled to meet the needs of virtually any organisation, capable of running hundreds to hundreds of thousands of workstations on one server.

As a consequence, fewer people are required to manage the system because it’s a smaller environment, and more simplified than running a string of different products and components across a number of locations.

As for the savings, a Gartner study published in 2008 estimated that “well-managed” desktop PCs could help cut TCO per year for those PCs by upwards of 40 per cent<sup>8</sup>, when compared to an unmanaged ones. Magnify that by several thousand desktops across the UK public sector and the savings become increasingly significant.

And while some system-wide IT desktop solutions can take several months to implement, this solution can be done, even in a big environment, in under a month. In some cases, this can be cut to a couple of weeks or even a week.

All of a sudden, the simple act of auditing its IT desktop environment seems like the most cost-effective thing the UK public sector could do.



## WHERE NEXT?

To see some of IBM's recent thinking on accomplishing more with fewer resources, visit IBM's public sector web pages at [www.ibm.com/easyaccess/publicuk](http://www.ibm.com/easyaccess/publicuk) where you can download some of the latest white papers:

### Rewriting the Rules of Patch Management

Commercial operations cannot continue to rely on the weekly or even monthly patch cycle that most of the public sector use at the moment. IBM can help protect customer services, corporate and customer data and day-to-day processes.

### Maintaining Continuous Compliance – A New Best Practice Approach

IBM offers auditing capabilities and visibility solutions and can assist in integrating with existing internal auditing practices. Application and vulnerability security solutions from IBM are industry leading.

### Smarter, Faster Endpoint Management Through Automation and Innovation

IBM services can help organisations drive up return on investment via better use of infrastructure. Having visibility, control and automation across your business enables you to better achieve your objectives and maximise asset value.

To find out how IBM's expertise can help, contact:

#### Steve Dudman

Tivoli Automation Sales for Central Government  
IBM Software Group  
M: +44 (0)7921 108020  
E: [dudman@uk.ibm.com](mailto:dudman@uk.ibm.com)

## References

1. <http://www.cio.co.uk/news/3244802/g-cloud-will-save-12-billion-says-john-suffolk-government-cio/>
2. <http://www.computerweekly.com/Articles/2009/07/29/237078/MPs-sceptical-of-16326.5bn-of-Gershon-IT-savings.htm>
3. <http://www.cio.co.uk/news/3244802/g-cloud-will-save-12-billion-says-john-suffolk-government-cio/>
4. <http://www.cio.co.uk/news/3244802/g-cloud-will-save-12-billion-says-john-suffolk-government-cio/>
5. "Deploy Critical Multi-Platform Updates in Minutes with BigFix Patch Management". White paper. BigFix
6. "Deploy Critical Multi-Platform Updates in Minutes with BigFix Patch Management". op cit
7. "Getting back to basics on patch management", Gartner Research, August 24, 2009 (document G00170521)
8. "Gartner Says Effective Management Can Cut Total Cost of Ownership for Desktop PCs by 42 Per cent". Gartner. March 10, 2008. <http://www.gartner.com/it/page.jsp?id=636308>



© Copyright IBM Corporation 2011

IBM United Kingdom Limited

PO Box 41

North Harbour

Portsmouth

Hampshire

PO6 3AU

The IBM home page can be found on the internet at [ibm.com](http://ibm.com)

IBM, the IBM logo and [ibm.com](http://ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries.

A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

Copying or downloading the images contained in this document is expressly prohibited without the written consent of IBM. This publication is for general guidance only.

Produced in the United Kingdom

March 2011

All Rights Reserved

Recycled fibre content 50% post consumer waste, 25% pre consumer waste and 25% virgin fibre.