WHITE PAPER

THE IMPACT OF MOBILE DEVICES ON THE SECURITY OF **CORPORATE IT SYSTEMS**

Contents.

EXECUTIVE SUMMARY

As the modern workplace grows into an increasingly fluid and fast-paced space, many workers are turning to portable and mobile devices to stay flexible and productive.

Business has evolved from office hours to an 'anytime, anywhere' schedule. As workplaces focus more on virtualisation, connectivity and cloud computing, it is integral for commercial success to engage with a fresh, more collaborative way of working.

Compared to two years ago, twice as many employees are logging onto corporate systems with the same personal devices that they use to access their social networks. This may seem like an encouraging sign of an increased work ethic but it also presents a massive security risk, as the business network becomes only as secure as the device in question. Meaning, theoretically, that a single lost phone could lead to confidential corporate information being accessed by multiple unknown parties.

According to Forbes magazine, "mobile app development projects will outnumber native PC projects by a ratio of 4-to-1"[1] by 2015.

"Theoretically, a single lost phone could lead to confidential corporate information being accessed by multiple unknown parties."

'Bring Your Own Device' – when employees bring personal devices into the workplace – is now unavoidable. It's virtually impossible to discourage employees from 'switching off' when at home or on-the-move.

With this in mind, it is essential that IT businesses establish stronger security awareness around the B.Y.O.D. space. Companies must focus on limiting and managing the risks that come from the use of personal devices. They must move with the times, rather than against them. It is integral that businesses work as safely as they can with the increasing use of mobile devices in the workplace.

"Mobile app development projects will outnumber native PC projects by a ratio of 4-to-1"[1] by 2015."

[1] Forbes Magazine, 'Mobile Business Stats for 2012', 2012

annodata
wider choice, better advice
A KYOCERA GROUP COMPANY

www.annodata.co.uk

IDENTIFYING AND COMBATING SECURITY THREATS

A global survey shows that almost 89% of IT professionals own mobile devices that connect to their corporate networks[2]. With the number of employees who use personal devices to work on-the-move increasing rapidly, the risk to company security continues to grow.

Nonetheless, it is increasingly difficult for the enterprise IT manager to maintain a standardised IT security policy. Often employees bring their own technology to the workplace, combining the personal and professional on one device. This blurs the lines of IT control as personally-owned devices are not governed by the same legal policies as standard-issue company technology.[3] These increasingly common circumstances only serve to highlight the numerous security challenges facing modern businesses.

Threats to corporate IT security can be posed by a variety of sources. These are not exclusive to employee use of personal devices, but can also include:

- Increased use of social media sites which increase the risk of data theft
- Malware threat on unsecured user devices
- Consumer cloud-computing services used for storage purposes
- Jail-breaking rooting devices on personal mobile phones
- Data being lost or damaged due to user error Data falling into wrongs hands if devices are lost or stolen.

Previously, the simple solution was to block these applications. There are many software programs available that will limit the amount of applications a user can access. Large corporations, however, have discovered employees are finding ways to 'cheat' these blocking mechanisms.

> "Personally-owned devices are not governed by the same legal policies as standard-issue company technology."

[2] Dimensional Research, 'The Impact of Mobile Devices on Information Security – a survey of IT professionals', 2012

[3] Pricewaterhousecoopers, 'Managing Security in a Mobile World', 2012

HOW TO DEVELOP ENHANCED SECURITY AROUND THE USE OF DEVICES

To counter these risks, many companies have begun developing targeted protocols alongside additional layers of management and security. This has led to the necessity of a BYOD policy for corporate networks. Occasionally, companies have begun to operate a 'token BYOD' – where less than ten percent of employees, mainly C-level executives and above – are allowed to connect their private devices to the network.

In the modern environment, 60% of employees believe that they don't need to be in the office to be efficient.[4] The use of tablets, mobiles and portable devices has and will continue to grow – as real-life consumer trends are diversifying the technology used in the workplace. This leads to employees questioning the relevance – or simply being ignorant - of IT policies.

Careless employees are regarded as a greater danger to business security than malicious hackers.

> "Malware targeting smartphones and tablets rose by 273% during the first half of 2011."

Employers must create strong, well-communicated policies regarding the boundaries of information security and disciplinary procedures for breaches of these policies.

Given that malware targeting smartphones and tablets rose by 273%[5] during the first half of 2011, it's increasingly important to have a strong, well-maintained IT infrastructure. Make use of Mobile Application Management – it provides a corporate app store that authorizes which applications employees can use. Whether managing or protecting against specific applications – from mobile-browsers to e-mail clients – this guarantees a timely mobile operating-system and remotely wipes lost devices, safeguarding against misappropriated information.

> "60% of employees believe that they don't need to be in the office to be efficient."

[4] http://newsroom.cisco.com/dlls/2010/ts_101910.html

[5] Pricewaterhousecoopers, 'Managing Security in a Mobile World', 2012

BENEFITS OF A PROFESSIONALLY MAINTAINED IT INFRASTRUCTURE

Having a well managed and professionally maintained IT infrastructure means understanding the devastation caused by having your systems and/or mobile devices compromised, damaged or found in the wrong hands. Well managed IT infrastructures are backed-up and protected from these real and costly harms.

When choosing an IT services provider, consider how current IT managers can ensure stored or transmitted data is inaccessible to unauthorised individuals. Businesses must ask themselves: are we safely providing employees access to all the resources they need from any device? Are our IT teams able to detect and address any intentional or unintentional changes made to transmitted or stored data? The best way to minimise security risks to your company is to invest in the strongest possible IT infrastructure.

A SUCCESSFUL IT INFRASTRUCTURE WILL:

Manage, protect and secure data on mobile devices used to access business information.

- Back-up business data to prevent data-loss
- Assess how mobile devices and applications holding data are used by employees
- Install robust anti-virus and firewall software to protect against phishing and malware
- Ensure devices are encrypted to safeguard business information
- Install customised operating systems by configuring and determining secure applications
- Provide definitions and policies for users regarding mobile devices.

SAFEGUARD YOUR BUSINESS WITH TAILORED IT SOLUTIONS

BYOD is the shape of the modern working environment and the "single most radical shift in the economics of client computing for business since PCs invaded the workplace"[6] Thus, it is key to integrate BYOD into your existing IT network and learn how to integrate these solutions without exposing yourself to unacceptable risk.

By investing in total system security management, businesses will be able to insure themselves against the increasing and inevitable use of mobile devices in the workplace.

CASE STUDY

If you are interested in how Annodata can provide tailored solutions to companies that use a blend of IT technologies, then have a look at the Plastic Omnium case study.

WHITE PAPER

You may also be interested in the white paper Managing Complex Bids in a Short Time Frame which looks at how working closely with a solutions provider will provide businesses with innovative, customized IT solutions.

[6] Gartner, David A. Willis, 'Bring Your Own Device: New Opportunities, New Challenges

Annodata is one of the UK's longest standing providers of Managed Services, covering Document Management, Unified Communications and IT.

For more information on how Annodata can help you become a more efficient enterprise, please contact:
marketing@annodata.co.uk or Tel: 01923 333 333

annodata
wider choice, better advice
A KYOCERA GROUP COMPANY

www.annodata.co.uk

v1 – Sept17