Monkey See - Monkey Take Photo: The Risk of Mobile Information Leakage

Karen Reanud, School of Computing Science, University of Glasgow, Glasgow, UK
Wendy Goucher, University of Glasgow, Glasgow, UK

ABSTRACT

Mobile devices have diffused through the global population with unprecedented rapidity. This diffusion has delivered great benefits to the populace at large. In the third world people living in rural areas are now able to contact family members who live in other parts of the country for the first time. For the city-dweller the mobile device revolution has brought the ability to communicate and work on the move, while they travel to and from work, or between meetings, thus making erstwhile “dead” time more productive. It is trivial, nowadays, to utilise workplace functionality, and access confidential information, outside the four walls of the organisation’s traditional boundaries. Data now moves across organisational boundaries, is stored on mobile devices, on USB sticks, and in emails, and also stored in the cloud. Organisations have somehow lost control over their data. This mobility and lack of control undeniably creates the potential for information leakage that could hurt the organisation. The almost ubiquitous camera-equipped mobile phones exacerbate the problem. These feature-rich phones change the threat from mere Shoulder Surfing into Visual Information Capture. Information is now no longer merely observed or overheard but potentially captured and retained without the knowledge of the person working on said documents in public. The first step in deciding how to manage any risk is to be able to estimate the extent and nature of the risk. This paper seeks to help organisations to understand the risk related to mobile working. We will model the mobile information leakage risk, depicting the factors that play a role in exacerbating and encouraging the threat. We then report on two experiments that investigated the vulnerability of data on laptops and tablet devices to visual information capture. The authors address both capability and likelihood (probability) of such leakage. The results deliver insight into the size of the Mobile Information Leakage risk. The following stage in this research will be to find feasible ways of mitigating the risk.

Keywords: Data Vulnerability, Mobile Information Leakage, Risk Management, Risk Mitigation, Shoulder Surfing, Visual Information Capture

1. INTRODUCTION

Mobile phones have diffused through the global population with breakneck speed (Middleton, 2007). It is predictable that they will be used in the workplace, especially with the significant recent improvements in their functionality over the last decade. Consider the fact that the popular mobile phone ten years ago was characterised by the ability to open up – the so-called clam...
shell phone was in great demand. However, a new era of mobile phone functionality was ushered in by Apple in 2007, with their release of the iPhone smart phone, a device that allowed owners to access the internet from their phones. According to Pew Internet1 (2012) 45% of Americans now own smart phones that can access the Internet and take photos.

The next step, using these devices to work while on the move was, perhaps, entirely predictable. Many 21st century employees work outside the formal office environment for a significant part of their working day (Worthington, 1998). Smart Phones have had a major impact on people’s working patterns and modalities and even on their travelling habits (Line et al., 2011). A report commissioned on behalf of the Chartered Society of Physiotherapists (Honan, 2012) reported that 65% continued to work on Smart Phones or other mobile devices once outside the office; working for an average of 2 hours 34 minutes in this way. This is made possible by the increasing capability of these devices and means that previously “dead” time spent travelling or waiting can now be utilised, enhancing employee productivity and maintaining the employee’s focus on business activities. This has changed in a very short space of time. In 2007, Lyons et al. carried out a survey of rail passengers in the UK, and the majority, back then, reported that electronic devices they carried did not improve the time they spent travelling. Fewer than 20% of their respondents reported working while travelling and only 20% of business travellers carried laptops. One could reasonably expect a very different response now, 6 years later.

Working on the move is seen as a positive trend by many organisations and their employees. Jain and Lyons (2008) write positively about the fact that travelling time can now be perceived as a gift rather than a pain. A number of surveys and questionnaires, including one by Good Technology, reported that 93% of respondents continued to work outside of the office, with 38% believing that their job would be impossible without at least mobile access to email.

There is surely a downside to all this mobile working. There are certainly concerns about the blurring of the home/work boundary and the balance between rest and work as work encroaches more and more on employee personal time (Gant & Kiesler, 2002). The other concern is that there is a risk associated with mobile working. There is a growing concern that workers will be observed while working on confidential documents on the move, and that leakage thereof could harm the organisation. In a recent survey conducted for Secure, The European Association for Visual Information Security2, 98% of organisations surveyed believed it was important to educate individuals on the observation threat and 32.4% said they had no confidence that users would make the effort to prevent information from being observed when working in public places.

That information does leak can be demonstrated by a two examples. Secure reports that the Vice President of an S & P 500 company took the time during her flight from London to New York to work on her company’s profit forecast for the following 6 months. Soon after she landed, a newspaper that was going to run a “Splash” on her forecast in the next day’s edition phoned her. A leak had come from the person in the neighbouring seat who happened to be a journalist. She had had plenty of time to appraise the information herself and to contact her paper with an analysis immediately upon landing.

In November 2008 a civil servant in the Department of Business fell asleep on the train while working on his laptop on documents marked with the security level ‘Restricted’. This event was captured photographically by a fellow passenger and led to a story in the Daily Mail newspaper (Owen, 2008). In the first case the information was merely leaked, in the second it was captured as well.

It is important to note that these were employees legitimately working on the move, on information they had a legitimate right to access. An observer exploited the situation, much in the same way as any social engineer might try to exploit the naivety of an employee.
E-Government and Creating a Citizen-Centric Government: A Study of Federal Government CIOs
www.igi-global.com/chapter/government-creating-citizen-centric-government/38383?camid=4v1a

Determinants of Terrorism in South Asia: Insights From a Dynamic Panel Data Analysis
www.igi-global.com/article/determinants-of-terrorism-in-south-asia/216877?camid=4v1a