In a World of Their Own: Working on the Move

Wendy Goucher & Karen Renaud
School of Computing Science
University of Glasgow
wendy@idrach.com, karen@dcsgla.ac.uk

The traditional model of white collar workers inhabiting offices to carry out their tasks is no longer valid in the 21st century. Many employees now carry information with them and work while travelling, in hotels and at home. This is a relatively recent development, however, and since the information they carry with them is often sensitive, we have to consider how this new model impacts on the security of the organisation's now distributed and potentially unsecured information. Whereas previously employees could relax within the company's office space, they now cannot let their guard down since they are surrounded by strangers who are not bound by the same loyalties or employment contracts. How aware are mobile workers of the risks of mobile working? Situational Awareness is a concept that has been well known since its role in the development in aircraft design following World War One. It continues to inform studies on the use of mobile phones in cars and the role of distraction in pedestrian accidents. This paper reports on research into leakage of sensitive business information that results from inattention to the risk of working in public places, while *on the move*.

Awareness, Security, Observation

1. INTRODUCTION

Organisations are justifiably concerned about information being leaked to unauthorised people. Leakages are often blamed on inadequate organizational processes (7), but this is a simplistic perspective. Another perspective was advanced by von Uexküll (10), who developed the idea of Umwelt, the *self world*, in which people perceive their environment subjectively. Hence each actor in a shared environment would have a distinctly different perception of the environment, and the risks related to particular activities. We could refer to this as a *virtual booth*: an invisible boundary between ourselves and others within the same environment. If Umwelt *does* exist, then one would expect to find a number of people with a variety of different perceptions of the necessity of the work and the risk related to carrying out the work in a public environment.

Consider the 21st century worker and how their modern working practice differs from that of the worker from the early 20th century. The modern worker has a less clear cut boundary between work and leisure (11). Many employees do the majority of their work away from a formal desk: whether working while travelling or from home. This, in turn, means that they carry information with them, a proportion of which is likely to be confidential or business sensitive. Information is therefore no longer secured

within one particular location: like the employees' working practices, it too is dispersed more widely than the brick and mortar organizational space.

Given the fact that the information is made available by dint of an employee openly accessing it in public and other unsecured areas, and that conveyors of such information possibly experience von Uexküll's *self world* concept, information leakage becomes not only understandable, but inevitable. Section 2 discusses related research in this area. Section 3 outlines a study carried out to assess the scale of the problem. Section 4 presents the findings and Section 5 concludes.

2. BACKGROUND

The situation whereby a person works in a public space with no apparent concern as to the potential for information leakage is one that is widely reported, albeit anecdotally (15). Some observers, in terms that hark back to that description of Thomas Aquinas, report people unwittingly leaking information as being in a '*world of their own*', so apparently oblivious do they seem of the risk of data leakage. There is a sense that they become unaware of their situation.

Sarter and Woods (9) define situational awareness as "*The accessibility of a comprehensive and coherent situation representation which is continuously being updated in accordance with the results of recurrent situation assessments*"

In the context of this research *situational awareness* defines the degree to which a person is aware of his or her immediate physical environment when concentrating on another task. The Sarter and Woods study examined the situational awareness of fighter pilots dividing their attention between close attention to instrumentation and the surrounding area that they are flying in. This area of research was a key stage in the study of situational awareness. Although the concept been studied formally since planes were first used in combat in World War One (1) the greater body of research began with the increasing speed of fighter jets and the demands on air traffic control to monitor and protect them. While it is undeniable that there are significant differences between the circumstances whereby a highly trained jet pilot evaluates all the information required to carry out their task, and the person working on a range of tasks in a public area with no particular training, there are sufficient similarities in the requirement for focused concentration in circumstances of significant distraction to allow some parallels to be drawn.

More recent research has focused on the possible distraction of car drivers who must divide their attention between driving and additional distractions such as the use of mobile phones. Lamble *et al.* (4) found that detection was impaired by up to a second in terms of time to collision when the driver was carrying out a non-visual task such as using a keypad while driving. Insurance companies in the UK and US have recently become interested in research carried out into the possible distraction of pedestrians using portable devices while they are moving because of the increasing incidence of accidents where device use is a factor. Madden (5) found that 17% of mobile phone owning adults reported having bumped into a person or obstacle as a result of talking or sending text messages on their phones. The degree of distraction was further investigated by Nasar (6) in locating objects for participants to pass while engaged in mobile phone conversation or using devices. He concluded that such devices presented a real risk to users' safety. There was little evidence that these pedestrians were aware of the risks related to their activities.

2.1. Umwelt

The fact that the person leaking sensitive information appears unaware of the risk of interception raises the possibility that they are distracted or perceive there to be no reason to take care of their

information transmission. If we in some way expect the sender to have some risk awareness that they do not then that awareness may vary from person to person. The idea that a person's perception of risk might vary from person to person lead to consideration of the how perception of risk might be constructed. In investigating this the concept of *Umwelt* emerged. Uexküll (10) asserted that every creature has their own subjective awareness of their immediate surroundings which could be described as their *phenomenological world*. Uexküll applied his concept to all living creatures, not only to humans, in order to gain insight into their behaviour. Although this is an old study it did, in its own way, break new ground in understanding the individuality of personal perception and the reasons behind it. Umwelt is informed by the individual understanding, experience and interpretation of the creature, or in our case, the person. Whereas other research in this area has focused on situation awareness, i.e. determining how absorbed people are in their current task, the umwelt perspective gives credibility to the idea of differing perspectives of the risks. Umwelt argues that perception is subjective and therefore awareness is not so much focused on another task as not including the awareness of information being intercepted by others. This idea precedes electronic distractions, such as those which may be the cause of the recent rise in accidents suffered by pedestrians while interacting with their smartphone. The idea of being '*Lost in Thought*' has been frequently applied, often to noted scholars and, indeed, was commonly observed in the behaviour of St. Thomas Aquinas in the 13th century (3), who was said to walk around the gardens lost in his thoughts and oblivious to the summons from passers by. Umwelt can release us from the concern about the role of the device to the wider picture of the cognitive absorption of the sender, as being separate from the focus of the person's attention.

While the device will undoubtedly play a role, it is clearly not the sole cause of this lack of awareness. Umwelt was further developed by Rappaport (8) who included the concept of the *cognitised environment* in which the individual's understanding and interpretation is filtered through the individual's motivation to observe and collect that information. When a person works in public the motivation to work might well be strong enough to lead them to discount the potential threats to the risks of engaging in that activity in a public environment. If, however, they fear that they may be overheard and therefore suffer some serious consequences, such as was the message of the famous World War Two posters using the tag line *Careless Talk Costs Lives* then the behaviour might be modified.

Figure 1: Information leakage Depiction. Both sender and a receiver are affected both by their context, (physical and psychological), and inhabit a virtual booth

Figure 1 depicts the information leakage situation. On the left is the *sender* who leaks information. There are two key factors which affect the behaviour of the sender:

- Firstly their awareness, both of the sensitivity of the information and the risk they are exposing the data to.
- Secondly there is the issue of context which is both the physical environment and the level of motivation they have to carry out the work.

The *receiver* is not represented as a personification as it could be the device the sender is interacting with or a person at the other end of a phone call. The receiver could also be the sender if the sender is reading a document and not realising that it is visible to others. The information is leaked to the *observer* who is the passive witness to the leakage.

Senders are influenced by their awareness, both of the information and the importance or sensitivity of that information.

Anecdotal tales of leakages are common but generally remain in oral tradition, with the consequent potential for corruption of the true nature of the circumstances that is inherent in that method of data storage. We therefore conducted an observation study to determine the extent of the problem.

3. OBSERVING RISK AWARENESS

There are clear ethical issues with collecting evidence of information leakage. Observers are usually unwilling recipients of leaked information, but often trapped by their circumstances into receiving it. For example, they could be on a train journey, waiting in an airport lounge or serving a customer in a restaurant. This project aimed to gather information about people's experiences of information leakage

without encouraging them to behave unethically. A key element of the design of the project, therefore, was the clear directive as to the information required, and by extension, the information that was not required.

The exercise aimed to record evidence of:

- The general circumstances of the leakage by category eg. on a train, in a restaurant etc.
- General characteristics of the sender e.g. gender, age, area of profession or work if obvious and relevant.
- The type of information leaked, e.g. financial, personal or business.

Given the potentially sensitive nature of leaked information it was clear that the observation exercise required careful design in order to avoid four potential problems:

1. The *Hawthorne effect* (12) whereby observers might play a pro-active role in encouraging information leakage.
2. The *social desirability effect* (14) whereby participants might make a particular effort to find examples of leakages in order to return positive results and thereby please the researcher.
3. Subjective interpretations of what what was required could lead to an *observer bias* (13) in the situations and information that were deemed to be appropriate for the purposes of the study.
4. It was crucial that volunteers did not feel that they were required to *spy* on those around them or even proactively to seek out information leakage situations.

Six volunteers were recruited initially. These were friends of the author and were approached directly; One was a retired person, one worked in the hospitality industry and the others were business consultants, mostly from small firms. It was felt to be important that volunteers (hereafter called observers) were explicitly instructed not to record any details of the leaked information. Each observer, was given a log book, called an *Observation Log*, to guide their reporting of the incidents, with spaces for each of the identified categories of interest. Only a small amount of additional space was left for comments in order to discourage observers from recording the actual information leaked. Observers were advised that they should only report incidents that took place in public. Information that might be gathered by visitors to company's own premises,

or from inadequate screening of devices within an organisation, are outwith the remit of this pilot study and are expected to remain so. The pilot ran for one month and served to highlight issues for consideration in designing subsequent studies.

As this was the first attempt at gathering information. Feedback gathered from observers on the nature and difficulty of their task was particularly important. Indeed, it was found that the low rate of incidents reported was partly explained by the unsuitability of the observer log method of recording. The following reasons were the most commonly cited:

- Observers, having volunteered, then found that they went through a period of infrequent travel or other exposure to areas later identified as hot spots. They felt that they were unable to fulfill their commitment, which left them feeling dissatisfied.
- Participants found themselves conflicted about carrying the log. Carrying it was often inconvenient but not doing so made them feel they were not fulfilling their commitment.
- Misunderstanding of the kind of incidents to be reported was common. One observer was very diligent in reporting conversations she had overheard in various situations. However, the observations were not directly helpful since they had attracted her attention because they were amusing, rather than because sensitive information was being leaked. This highlights the observer bias that was identified at the outset.

The following section presents the findings from the first stage of the project.

4. FINDINGS

A number of findings emerged from the participants' reports:

- A wide variety of media of data leakage in a range of environments were identified.
- *Hot spots* were identified where leakage was more commonly observed.
- The observed, referred to as 'The Sender' commonly appeared oblivious to the monitoring of their information.
- Observers reported increased awareness of their own potential information leaking behaviours as a result of participation.

We subsequently sought to address some of the issues raised by observers and recruited more

participants for the second study. All participants volunteered directly, after explanation of the project in one to one context or as part of an industry conference workshop. This time all were business people as the trial project had shown that group to have a higher rate of reporting, possibly due to their greater mobility. This time observers were directed to use the *Spontaneous Reporting* method. The observers were fully briefed as to guidelines of required information and then were to make contact with the researcher by email or text to give basic details of observed incidents as and when, or if, they occurred. Observers then signed a consent form, which had been approved by the University ethics committee, to show their understanding of the requirements of the exercise. This approach is still in its early days, as this paper is written, but even at this point there is an increase in the number and variety of incidents reported, including from countries outside of the UK.

4.1. Working in Public

Even at this early stage a variety of incidents have been reported. However, the use of business people as observers in the more recent stage seems to have concentrated the nature of the information to the business-focused. It is too early to conclude that is due to selection bias or due to the nature of observers' exposure, or other causes. The strong briefing regarding the non-reporting of sensitive information has, so far, been successful and no reports have included examples of actual information leaked. It is worth noting, however, that one of the benefits of *Spontaneous reporting* is that it gives observers the opportunity to get near real-time feedback, and, if necessary, corrective direction, should sensitive information be reported.

4.2. Hot Spots

Leakages were identified in a range of situations. However, many occurred in hospitality and transportation contexts. Incidents most commonly presented where people were seated at a table on trains or in airports or on planes. In those cases there were often a combination of leakage from open laptop use, sensitive papers on clear display and from conversations on mobile phones. Anecdotal evidence received at the planning stage of this project suggested that there would be a significant amount of data leakage in restaurants and bars. While these contexts have not been specifically targeted, some incidents have indeed been reported from such environments. In one incident a customer sat alone at a bar in the daytime working on her laptop; the observer reported "*A lady was sat by the bar preparing year-end results and forward projections for [A well known soft drinks manufacturer]*". She had her laptop

open with the spreadsheet, from which she spent some time devising the appropriate diagrams.” The incident happened in a city where a high proportion of bar staff are recent graduate, or undergraduate, students, many of whom are likely to have some knowledge of business and economics and therefore understand the leaked data.

4.3. Verbal Leakage

These have been less common than expected. Indeed, most examples thus far related to the leakage of personal data. Generally this was financial, with credit card details most commonly leaked. One, observed in a restaurant, consisted of a businessman discussing a range of sensitive business information, including strategy and revenue for his well known employer, during an overheard mobile phone call. There were also a instances of face to face discussions leading to the leakage of business, and other sensitive data mostly concentrated in coffee shops and bars.

4.4. Shoulder Surfing

Shoulder surfing occurs when information is gathered by covert observation (2). Reports indicate that this is more common on trains, planes and in airport lounges. The common denominator appears to be those places where the sender anticipates being in one place for a while and so that they can focus on a particular task. Leaked information ranged from e-mail to browser pages to payment pages for retail transactions and business reports. Leakage was mostly, but not exclusively, from laptop screens. Two examples reported The first example was e-mailed in real time from a train journey *“I am sitting next to someone on the train who works for [A well known international consultancy] and he’s got his laptop out...I can see his screen! He has [the company] logo on his desktop and he has been going through an expenditure review for a client.”* As new ‘tablet’ devices emerge, with ever clearer screens that can be viewed with ease, but protected less readily, the need for the user to understand the risk of using these devices to work on sensitive material appears to grow too.

4.5. Examples of Reports

In one incident the observer, herself a solicitor, reported: *“I read an entire barrister’s brief about a child’s case whilst sitting opposite to him on the train”*. Another incident took place on in busy commuter train between Madrid and Barcelona. The *sender* was using his laptop in clear view of those around. An Excel spreadsheet was being worked on and the observer reported being able to see details of revenue for the organisation and a

full 2010 year profit and loss account was visible for most of a 2.5 hour journey. Another example took place on the commuter train from Madrid to Barcelona February 2011. *“He is having a 20 minute conversation over the phone with a problem he’s having with a colleague. He’s explaining in detail (with names and organizational issues) the problem. I could easily figure out the company and I already know the names of people involved.”* It was highly probable that at least some fellow passengers could identify the company being discussed. Some might even have been customers.

4.6. Discussion

There was a positive expectation, at the beginning of the project, based on existing anecdotal evidence, that it would be possible to gather some examples of incidents of data leakage. Indeed that has proved to be the case. It has also, however, begun to reveal some of the factors that impact on the behaviour of both the sender and the observer in terms of the actions they take and the risk acceptance that is part of the process. The most surprising finding of this project was the discovery of the *Awareness Reinforcement Loop*. Figure 1 has been modified to include this, as represented by the arrow between the *observer* and the fall in their Risk Acceptance level (Figure 2). This demonstrates the reported change of the observer’s perceptions with regard to their own potential for information leakage when working on the move. One observer reported *“I now don’t make or take business calls on trains other than perhaps to say I will call the person back and I don’t work on the train other than on non-contentious stuff.”* Another said *“As a result of being involved in this project, I am now much more careful about what I read on a PC or smartphone when in a public place , and what I say in public to others, particularly as I am a trustee on a board.”*

Given that people are often seen as the weakest link in the information security chain, one could expect many organisations to invest in security awareness programmes. Unfortunately the investment has been dropping proportionately over the last 3 years. The 2011 survey by Price Waterhouse Coopers found that fewer respondents, compared to last year, conduct security awareness programs. They argue that it is difficult to identify return on investment with regards to behaviour based improvements(16). While basing a security awareness program on encouraging staff to monitor the security leakage of their fellow commuter passengers would have ethical issues, results from this, and further, studies into this area could be used to inform that security awareness training that is required to fulfil industry compliance requirements such as ISO 27001

Figure 2: This diagram extends Figure 1 to incorporate the reinforcement loop

Given that the observations are based on behaviour it is reasonable to consider that there may be cultural difference in security behaviour (17) within the UK and in mainland Europe and North America. For that reason some of the volunteers were selected because they either travel outside the UK on a regular basis, or are based overseas. This has already resulted in a few replies that appear to indicate that the *Virtual Booth* phenomenon is also apparent outside the British cultural influence.

5. CONCLUSIONS & FUTURE WORK

The proliferation of increasingly compact and powerful electronic devices has meant that the long-known phenomenon of someone becoming so engrossed in their work that they are oblivious to risks of loss or leakage of the data is now a growing business problem. Business people are ever more mobile in the course of their work. Advancing technology means that there is, in effect, little difference between the technological facilities available to work at the desk or on the move. This study revealed instances of insecure working in a range of situations and using a number different types of media. A key finding of this work is that some volunteers who reported instances of data leakage claimed that their own risk acceptance had lowered and they were being more cautious about the work they were willing to do in a public arena. This demonstrated that raising awareness about the potential accessibility of data when working in public, even by casual, none technical, means lead to them taking more precautions and therefore a probable improvement of the security of the material they might work on.

This being an early stage project there are a number of different areas of development that are suggested by the information so far gathered. Further examples will be gathered, with particular

emphasis on observation outside of the UK to attempt to isolate this phenomenon from any cultural influence. There are also a number of directions that could be taken that will bring greater understanding of the background to the Virtual Booth in terms of identifying existing ideas and in research and experimentation of behaviours so far identified.

6. REFERENCES

- [1]Mica.R. Endsley. Towards a history of situation, 1995.
- [2]European Network and Information Security Agency. ATM crime, 2009.
- [3]Nicholas M. Healy. Thomas Aquinas: theologian of the Christian life. Ashgate Publishing Limited, 2003.
- [4]D Lamble, T Kauranen, M Laakso, and H Summala. Cognitive load and detection thresholds in car following situations: safety implications for using mobile (cellular) telephones while driving., November 1999.
- [5]Mary Madden and Lee Raine. Adults and Cell phone distractions, 2010.
- [6]Jack Nasar, Peter Hecht, and Richard Wener. Mobile telephones, distracted attention, and pedestrian safety. Accident; analysis and prevention, 40(1):6975, January 2008.
- [7]Price Waterhouse Coopers. Data loss prevention: Keeping sensitive data out of the wrong hands. Web Document, July 2008.
- [8]Roy A Rappaport. Pigs for the Ancestors. Ritual in the Ecology of A New Guinea People. Yale University Press, 1984.
- [9]N.B. Sarter and D.D. Woods. Situational Awareness: A critical but ill-defined phenomenon. International Journal of Aviation Psychology, 1:4557, 1991.
- [10]Jacob Uexkull. A stroll through the worlds of animals and men. In C Schiller, editor, Instinctive Behavior. International Universities Press, New York, 1934.
- [11]Judy Wajcman, Michael Bittman, Lynne Johnstone, Jude Brown, and Paul Jones. The Impact of the Mobile phone on Work/life balance, 2008.
- [12]Franke RH, Kaul JD: The Hawthorne experiments: First statistical interpretation. Am Sociol Rev 1978 , 43:623-643
- [13]Jones, E. E., and Nisbett, R. E. (1971). The actor and the observer: Divergent Perceptions of the Causes of Behavior. New York: General Learning Press.
- [14]Paulhus, D.L. Two-component models of socially desirable responding, Journal of Personality and Social Psychology 46 (1984) (3), pp. 598609.
- [15]Gustin, M. Overheard at the Throwdown: Houston's version of Iron Chef is where food secrets come out. 27 July, 2010. CultureMap Houston.
- [16]Goucher, W. The glamour of the shiny box solution Computer fraud & Security published by Elsevier. November 2008
- [17]Ross, Steven Creating a culture of security. ISACA Rolling Meadows II USA. Publication expected April 2011