ICT professionals' perceptions of responsibility for breaches of computer security

Professor Mary Barrett
School of Management & Marketing, University of Wollongong, Wollongong, Australia
Email: mbarrett@uow.edu.au

Dr Karin Garrety
School of Management & Marketing, University of Wollongong, Wollongong, Australia
Email: Karin@uow.edu.au

Professor Jennifer Seberry
Centre for Research in Computer Security, University of Wollongong, Wollongong, Australia
Email: Jennifer_seberry@uow.edu.au

ICT professionals' perceptions of responsibility for breaches of computer security

ABSTRACT

With ubiquitous computer use and networking, concerns about security breaches have intensified. However the human element in security, especially perceptions of responsibility, is less well understood than technological solutions, and both are needed. Previous studies focus on 'regular' users rather than ICT specialists. This paper reports on a scenario-based survey of ICT professionals comparing their views on responsibility for typical and serious computer security breaches with what they believe senior, non computer-skilled managers believe. Results showed that ICT professionals are actually tougher on themselves than they think management would be and regard computer security as 'their job', yet feel misunderstood and under-appreciated in their organisations. The paper discusses potential organisational problems arising from this contradictory stance and suggests further research.

Keywords: ICT professionals, computer security, breaches, responsibility, organisational culture, work

Computer security – a growing problem

The security of information that is held on computers has been a matter of concern for decades. With the spread of networking and ubiquitous computing, concerns about security have intensified (Lampson 2004, Thomson & von Solms 1998). The theft of account numbers and passwords over the internet can lead to theft of personal identity – someone can BE someone else. Viruses play havoc with computer systems, leading to loss of valuable data and costly time spent on repair. The threat of terrorist attack is increased when terrorist groups gain access to sensitive information. In response to these and many other security concerns, computer technicians have devised a plethora of technical procedures designed to protect the integrity of information. These include checklists, access control lists, firewalls, anti-virus software, passwords and encryption protocols (Lampson 2004, Siponen 2005).

Given the amount of effort that has been expended on technical devices and procedures for establishing and maintaining computer security, we would expect that information in most organisations is adequately protected, with only authorised users gaining access to it. However, this is not the case. Many IT specialists have pointed out that computers systems are, in general, much less secure than they could or should be (Lampson 2004, Straub & Welke 1998). Why is this so? Increasingly, writers in the field of computer security have argued that, in order to close the gap

between what is theoretically possible and what occurs in practice, we need to shift our focus away from the purely technical, and develop a deeper understanding of the human-computer interactions through which effective security is – or is not – established and maintained. There are a number of ways that theorists have incorporated human elements into their analyses of responsibility for computer security, each of which generates suggestions for improvement.

Accounting for human responsibility in computer security breaches: training weaknesses, culture or responsibility structures?

Training weaknesses? One argument about why security measures remain weak is that the people who commission, design and use computer systems are not adequately trained. In this view, security can be improved by educating users and employees in organisations where sensitive information is gathered, stored and exchanged (Hentea 2005, Straub & Welke 1998, Thomson & von Solms 1998). For example, Straub and Welke (1998) conducted an action research project in two Fortune 500 companies. They found that although managers had 'an overwhelmingly positive attitude toward security', this 'was not accompanied by thorough understanding of available security responses' (p. 456). As part of their project, they provided training in security risk analysis and planning, which the managers incorporated into their procedures. However, while such education is undoubtedly critical for improving security, knowledge and awareness do not necessarily translate into effective actions. In everyday work situations, computer users are often subjected to conflicting demands. Although they may 'know' that security is important, they sometimes ignore or circumvent security measures when they complicate or delay the task at hand (Dourish et al. 2004, Fisk 2002, Lampson 2004). In addition, while this work focuses on the complexities surrounding computer security for 'regular' users, ie non ICT staff, we still know little about how these demands may affect the work of ICT professionals themselves.

Culture? One way of bringing the broader work context into considerations of computer security is to focus on those aspects of organisational culture that facilitate and/or hinder effective security practices. Work carried out from this perspective emphasises how employees' actions are influenced by organisational norms, beliefs and expectations. Although formal training may transmit information about security procedures and their importance, localised cultural and sub-cultural practices may

include tolerance or even encouragement of insecure practices (Chia et al. 2002, Kessler 2001, Siponen 2001). In order to establish and maintain effective security, the informal norms, beliefs and routines of organisations need to be engineered so that they are in line with specified security requirements. This type of change, however, is typically difficult to achieve.

Responsibility structures? Another more pragmatic way of understanding why computer security breaches happen is to bring the broader work context into considerations of computer security, by investigating its structural as well as cultural components. There is a promising strand of work along these lines that examines how responsibilities for computer security are, or should be, distributed within and across organisations (Dobson 1991, Strens & Dobson 1993, Thomas & Sandhu 1994, Hitchings 1996, Backhouse & Dhillon 1996, McDermott & Fox 1999, Takanen et al. 2004). In these studies, responsibility is not an abstract concept, but a concrete set of socio-technical activities carried out within specific relationships. In the words of Backhouse and Dhillon (1996, p. 5), 'structures of responsibility'

> provide a means to understand the manner in which responsible agents are identified; the formal and informal environments in which they exist; the influences they are subjected to; the range of conduct open to them; the manner in which they signify the occurrence of events; the communications they enter into and above all the underlying patterns of behaviour.

Ideally, by tracing these structures and patterns, analysts should be able to form a holistic view of the information system under investigation, a view which includes the relationships, technologies and procedures through which information is produced, exchanged, altered and protected. In this way, they can form connections between high level abstractions, such as organisational goals, and more low level concerns, such as the duties of particular individuals and the capabilities and limits of various pieces of equipment and software (Thomas & Sadhu 1994).

The 'structures of responsibility' approach to computer security is promising because it has the capacity to bridge the divide between the purely technical components involved in computer security and the socio-cultural factors that so heavily influence how people behave in organisations. However, the published work to date has tended to assume that structures of responsibility are stable and relatively easy to identify and map. Moreover, the maps that have been produced as illustrations of this

approach (e.g. Backhouse & Dhillon 1996 p. 7, Hitchings 1996 p. 6, Takanen et al. 2004, p. 100) appear to be formalised analysts' (normally ICT professionals') interpretations. The degree to which actors 'on the ground' concur or disagree with the analysts' interpretations of where responsibility lies is not clear. In addition, how ICT professionals see their own responsibilities in specific scenarios where they could be blamed for computer security failure, and how they think others will regard such failure, are also not clear. While attempts to investigate and map out structures of responsibility are a welcome development in the quest to include humans in our theories of how computer systems work, assuming that their patterns of activity and attributions of responsibility are clearly identifiable and stable neglects some important dimensions of human experience, namely, that activities, relationships and attributions of responsibility shift about and are often contested. As anyone who has worked in an organisation knows, managers, staff and ICT personnel often have quite different ideas about who is responsible for what. Moreover, these ideas shift about as colleagues cover for one another, engage in power struggles and search for someone to blame when mistakes are made.

In this paper, we explore some of these issues. We report findings from a study of computer security professionals which considers how different organisational members attribute responsibility for computer security breaches. The study was based on scenarios which asked for ICT professionals' views about the underlying causes of security breaches. We also asked them to predict how senior, non-ICT managers would view the same breaches. In this way, we sought to find out more about how ICT professionals, rather than 'regular', non-professional users, who have been the focus of earlier training, culture-oriented, or 'structures of responsibility'-oriented studies, see responsibility for computer security in particular situations, and how they believe responsibility for computer security is likely to be seen by senior, but non-computer expert, staff.

METHOD

The survey instrument

A questionnaire was drawn up consisting of three brief scenarios of computer security breaches. It also contained some questions about the demographics of the respondents and their organisations, and respondents' views on how much the need for good computer security is understood and supported in their organisations. The scenarios about computer security breaches were devised to reflect realistic,

even common computer security breaches, which have in the past led to major costs and inconvenience for the organisation in which they occurred, or even threats to national security. The questionnaire was piloted with members of the computer security community to ensure the realism of the scenarios, their possible consequences, and a plausible set of views about various parties' responsibility for them.

Administration of the survey

Participants, who were computer security specialists and also members of the Australia-wide Information Security Interest Group (ISIG), were approached by the researchers during two seminar days organised by ISIG in late 2005 and invited to fill in the questionnaire. The seminars took place in the CBD in Sydney and Brisbane. Following the Sydney seminar, the ISIG Annual General Meeting was conducted by teleconference, linking ISIG members in four other Australian capital cities. By arrangement with the ISIG executive, copies of the questionnaire had been sent to these other venues in advance of the teleconference for distribution to members. At the Sydney and Brisbane seminars the questionnaire and information sheet about the project were placed on participants' seats at the outset of the seminar. The study and the researchers were briefly introduced by the MC, and participants were invited to fill out the questionnaire and return it to the researchers sometime during the day. A total of 96 questionnaires were collected using these combined methods, approximately 25% of the total membership of ISIG.

RESULTS

Demographics

The overwhelming majority (88%) of respondents were male, with the dominant age group (45%) being 30-39 years. 14% were aged 19-20, 25% were aged 40-49, 11% were aged 50-59, with the remainder 60 years and over. 77% of respondents said they were employed in an organisation with a further 17% either self-employed or self-employed and also employing others. An analysis of the respondents' job titles indicated that all considered themselves to be ICT professionals. 20% percent were at the top of their organisations, with 23% at middle to senior management level and 36% at middle management level. The remainder were at the lower level (13%) or entry level (3%) of their organisations.

Results for Scenario 1

The first scenario read as follows:

> *A cadet member of staff in the ICT section in a major University is given the job of putting new materials onto the web for distribution. Being new to the position he does not realise that he has accidentally mirrored the whole site to the world wide web when he finishes his job. Eight months later, while doing a Google search, a senior member of the IT staff discovers that confidential documents – examinations, student data, tutorial solutions – have been available on the site to the casual reader during the entire period.*

There were four options for indicating who was to blame for the incident: a) the **Federal government** because universities' funding is being cut, meaning inexperienced people are being employed to do work that properly qualified ICT staff should do; b) **the University**, because it failed to have checking procedures to verify critical work by cadet staff; c) **the ICT supervisor**, because she failed to use common sense and check the cadet's work, and d) **the cadet**, for not asking for his work be checked.[1] For each scenario respondents were asked to use a five-point Likert-type scale to indicate a) the extent of their agreement with a series of statements about responsibility for the breach, and also b) what they thought a senior, non-ICT staff member in their organisation would think about responsibility for the breach.

Participants overwhelmingly believed the 'colleague at the next desk' would blame either the University or the ICT supervisor for the security breach, with 74% and 81% of participants saying a close colleague would agree or strongly agree with statements b) and c) respectively. They were less likely to believe that management would share this view, however, with statements b) and c) scoring 65% and 74% respectively for senior managers' likely opinions. Very few thought either a colleague or senior management (23%/20% respectively) would blame the Federal government. Only 21% thought a colleague would blame the cadet himself, though at 41% they are clearly concerned that senior managers might blame him.

[1] In addition, participants were invited to think of and then write down another explanation which would have been plausible in the situation. Analysis of these qualitative responses for all three scenarios is continuing. Finally, participants were asked to indicate which response they most agreed with, including any response they had written themselves. The analysis of this part of the questionnaire is also continuing.

Implications of scenario 1

Following a frequent technique in social science research, this survey first asked respondents to rate the responses to the scenarios 'as if' they were 'a colleague […] who has the same level and kind of ICT expertise as you'. This is thought to be a more accurate way of obtaining respondents' own views than asking the question directly, by reducing social desirability response bias. This means that the answers given on the part of 'a colleague' can be taken as the respondents' own views. This stance was adopted for all scenarios.

It is interesting that, more than blaming external parties such as the Federal government for inadequate resources or the University for inadequate procedures, respondents from the ICT community typically blame the ICT supervisor. It is also revealing that respondents believe a close colleague would actually be *more* likely to blame the ICT supervisor than they think senior management would. It is clear that information security staff take a strong view of their professional responsibility in this matter since they think a colleague would take a dim view of the ICT supervisor's lack of common sense. They are also concerned that the cadet would be blamed by management for the breach – a situation they would no doubt view as unfair given the cadet's limited experience.

Results for Scenario 2

The second scenario read as follows:

> *It is the year 2008. North Korea and the U.S., after many years' standoff, have finally agreed that North Korea may build a limited nuclear facility under the strict surveillance of United Nations inspectors. The first nuclear power station has been built and others are close to completion. Programming contractors have been given computer accounts in order to initialise the production of nuclear power. The contractors complete their work, are paid off, and leave. No-one ever removes their accounts. The CIA discovers, when they raid a terrorist cell in Middle East, that the terrorists had accessed the accounts in the North Korean nuclear power station because they were left active.*

There were again four possible responses to this scenario: a) **it wasn't the contractors' fault** because they didn't have the administrative privileges to close their accounts; b) **it wasn't the fault of the person who had the administrative privileges to close the accounts** because the job had been 'hush

hush' and not discussed with her; c) **it wasn't the fault of the manager of the nuclear power station** because it should have been taken care of by the ICT staff and the UN auditors; d) **top managers will ensure procedures are in place to ensure security** in sensitive organisations because of the awareness created by the incident.

Respondents believe a colleague wouldn't blame the contractors (81%), but are markedly less confident that senior management would feel the same way (58%). They place the blame on the person who had the administrative privileges to close the accounts (71% think a close colleague would *disagree* with statement b)), though again they are less sure (61%) that senior management would be as tough on the supervisor. Nearly as many (66%) as think a colleague would blame the person with account closing privileges also feel the manager of the nuclear power station is at fault. Only 50% of respondents thought a colleague would believe greater security measures would result from the breach, though they think senior management would be optimistic in this regard (77%).

Implications of scenario 2

This result echoes the result for scenario 1 in that ICT professionals typically do not blame outsiders such as the contractors, but are tough on the person in their own ranks – the person who had the administrative privileges to close the accounts. However now there is an additional element in play – a desire that management, in this case the manager of the nuclear power station, should also take responsibility for the problem. They are markedly more cynical in their views about whether there will be a 'silver lining' to the breach in the form of better security as a result of improved awareness, although they think senior management would think security would improve. Again, it emerges that ICT professionals see themselves as taking responsibility, but also feel that management should be both more aware of their role, and more convinced that 'better security' will not just happen automatically.

Scenario 3

The third scenario read as follows:

> *A disgruntled ICT employee who left his organisation in some bitterness, drops in six months later to visit his old friends in the section. While he is there, he manages to upload a virus which randomly deletes some files instead of saving them when the save command is invoked. The*

problem was initially ascribed to inexperienced casual ICT staff who had been working there for a period, or hackers. It was only rectified after months of inconvenience and a great deal of data had been lost.

The four possible responses to this scenario were a) **it wasn't the fault of the permanent systems administrators** (since it was reasonable to have thought the problems were caused by someone inexperienced, or a hacker, and they had no reason to suspect their former colleague); b) **it wasn't the fault of the ICT Department Manager** since the employees should have prevented the ex-staffer from being in a situation where he could upload a virus; c) **it is not reasonable for organisational budgets to include a major contingency element against computer security breaches**, since this should be everyone's responsibility; d) **the CEO would be justified in outsourcing all ICT security** since having an in-house security team is not an effective solution.

Again, the ICT staff are tough on the permanent systems administrators, with 79% saying a colleague would *disagree* that they weren't to blame. As in scenarios 1 and 2, they were actually tougher on this person from their own ranks than they thought management would be (64%). Again, however, they also felt that the immediate management figure in the scenario – the ICT Department Manager – should take some blame (61%). However they felt this person to be less strongly at fault than the permanent systems administrators, and this time they felt both management and their colleague would agree (60%). However they appear less sure that management will follow through on this shared view by providing budgetary and in-house personnel support for computer security. The majority (72%) believed a colleague would disagree that organisational budgets shouldn't include a contingency element for computer security, but only 39% thought a senior manager would disagree with this. Similarly, 73% disagreed that the CEO would be justified in outsourcing all ICT security, but only 32% thought senior managers would share this view.

Implications of scenario 3

As in the previous scenarios, ICT staff appear strongly prepared to blame any member of their own ranks who has acted unprofessionally or otherwise done something seriously wrong. However they feel 'misunderstood' in that they believe management would see a problem such as the one in scenario

3 as a reason to downsize, or even completely outsource, ICT security – a view they strongly disagree with.

Support for and understanding of the need for good computer security in respondents' organisations

Responses to the final four questions indicated that respondents are reasonably confident that senior managers and supervisors are highly aware of the need for good computer security (69% and 67% agreement respectively). However only 50% believe that ordinary employees are similarly aware. Moreover, this strong awareness on the part of management doesn't seem to be borne out in respondents' perceptions about how much support is available. Only 45% believe that adequate support (funds, training, etc) is made available in their organisations for good computer security to be achieved and 35% disagree that this is support is available.

GENERAL IMPLICATIONS AND FURTHER RESEARCH

Examining the responses to all three scenarios and the views about how much organisational support is available for computer security, suggests that the maps yielded by the structures of responsibility approach, although useful, need to be considered as general, rather idealised representations rather than a complete picture of responsibility for computer security. This suggests in turn that the findings of Dourish (2004) for computer users may apply to ICT professional staff as well as to 'regular' computer users, that is, that responsibilities are structured in part by the pressures of the organisational environment, time restrictions, and so on. One area of potential contradiction between representations yielded by responsibility structure maps and broader organisational realities is the divide this study showed between the perceptions of ICT professionals about how they do their job and how they see responsibility for it, and on the other hand how they believe their work is perceived by other parts of their organisations. While ICT staff seem to have a strong sense of their professional responsibility in relation to computer security breaches and are prepared to be tough on individuals from their own ranks whom they think have done a poor job of maintaining computer security, they also believe their work to be inadequately understood and supported both by ordinary employees, and also by those parts of management that could support their work by providing bigger budgets and training for

computer security at an organisation wide level. So computer security is paradoxically both ICT's job, and one that needs to be shared.

This is potentially a source of difficulty. Because they clearly take responsibility for computer security, ICT staff may knowingly or unknowingly give other staff in their organisations the idea that 'computer security is our job – leave it to the experts', which tends to decrease the likelihood that the responsibility will be shared. However, since the findings of this survey are based on perceptions drawn from ICT staff rather than organisational members generally, we need to ask how widely their views are shared in organisations.

This could be explored by looking at, for example, how social identity in computer work is constructed, since even with the rise in computer literacy generally, many computer issues including responsibility for security, may be thought of by non-ICT staff as 'other people's work' i.e. as the work of ICT staff. That is, non-ICT staff may construct their social identity in part by *excluding* computer work and responsibility for computer security. And, as mentioned earlier, ICT professionals may also to some extent construct their work identity around their expertise and authority in this area. Other factors may complicate the situation further. Employees may be unwilling to undertake 'security work' given an increasing awareness of organisations' capacity to engage in surveillance of employees. Developing successful strategies to manage these issues, eg through change to existing computer security strategies and related training, requires a highly nuanced appreciation of these issues.

We would suggest further research as follows: to see how widespread these contradictory views of professional responsibility are, further quantitatively focussed work using this instrument and perhaps others is needed, but gathering responses from non-ICT staff as well as ICT staff in one or more major organisations. Of course, perceptions of responsibility are closely linked to other issues, including professional identity. But perceptions of identity are more difficult to access without qualitative work, especially in-depth interviews. Accordingly, further research should include interviews with employees in the same or similar organisations as the quantitative work was done, to gather data about how employees (both ICT and non-ICT) construct their work identity, and the relationship of this to the distribution of responsibility for computer work and computer security. Focus groups or interviews

with both ICT and non-ICT employees and managers would provide suitable starting points. Other approaches are also possible. The results of this and later work could help improve awareness of computer security issues, help improve training strategies, and generally increase mutual understanding of ICT and non-ICT staff who work to create sound computer security.

References

Backhouse, James, and Gupreet Dhillon. 1996. "Structures of responsibility and security of information systems." *European Journal of Information Systems* 5:2-9.

Chia, P. A., S. B. Maynard, and A. B. Ruighaver. 2002. "Understanding Organizational Security Culture." in *Proceedings of PACIS2002*. Japan.

Dobson, John. 1991. "A methodology for analysing human and computer-related issues in secure systems." Pp. 151-170 in *Sixth IFIP International Conference on Computer Security and Information Integrity in our changing world*, edited by Klaus Dittrich, Seppo Rautakivi, and Juhani Saari. Helsinki, Finland: Elsevier Science Publishers.

Dourish, Paul, Rebecca E. Grinter, Jessical Delgado de la Flor, and Melissa Joseph. 2004. "Security in the wild: user strategies for managing security as an everyday, practical problem." *Personal and Ubiquitous Computing* 8: 391-401

Fisk, Mike. 2002. "Causes and remedies for social acceptance of network insecurity." Pp. 1-4 in *Workshop on Economics and Internet Insecurity*.

Hentea, Mariana. 2005. "A perspective on achieving information security awareness." Pp. 169 - 178 in *Information Science and Information Technology Education*. Flagstaff, Arizona, USA.

Hitchings, J. 1996. "A practical solution to the complex human issues of information security design." Pp. 3-11 in *Information Systems Security. Facing the information society of the 21st century*, edited by Sokratis K. Katsikas and Dimitris Gritzalis. London: Chapman & Hall.

Kessler, G. C. 2001. "Non-technical hurdles to implementing effective security policies." *IEEE ITPro Magazine (edited version)* March/April.

Lampson, Butler W. 2004. "Computer Security in the Real World." *Computer* June: 37-46.

McDermott, John, and Chris Fox. 1999. "Using abuse case models for security requirements analysis." Pp. 55-64 in *15th Annual Computer Security Applications Conference*.

Siponen, M. T. 2001. "A conceptual foundation for organizational information security awareness." *Information Management and Computer Security* 8:31-41.

Siponen, Mikko T. 2005. "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods." *Information and Organization* : 15 (4): 339-375

Straub, Detmar W., and Richard J. Welke. 1998. "Coping with systems risk: security planning models for management decision-making." *MIS Quarterly* 22:441-469. 167-173.

Strens, Ros, and John Dobson. 1993. "How responsibility modelling leads to security requirements." Pp. 143-149 in *Proceedings of the 1992-1993 workshop on new security requirements*. Rhode, Island, US.

Takanen, Ari, Petri Vuorijarvi, Marko Laasko, and Juha Roning. 2004. "Agents of responsibility in software vulnerability processes." *Ethics and Information Technology* 6:93-110.

Thomas, Roshan K., and Ravi S. Sandhu. 1994. "Conceptual foundations for a model of task-based authorizations." Pp. 66-79 in *Computer Security Foundations Workshop VII*. Franconia, NH, USA.

Thomson, M. E., and R. von Solms. 1998. "Information security awareness: educating your users effectively." *Information Management and Computer Security* 6: 167-173.