2007

Information and computer technology security: furthering the research agenda

Karin Garrety
University of Wollongong, karin@uow.edu.au

M Barrett
University of Wollongong, mbarrett@uow.edu.au

Publication Details

This conference paper was originally published as Garrety, K and Barrett, M, Information and computer technology security: furthering the research agenda, ANZAM, Sydney, 4-7 December, 2007.

Information and computer technology security: furthering the research agenda

Abstract
Despite the development of advanced technical devices and procedures, the information held in computer systems remains vulnerable to attack and/or inadvertent mishandling, resulting in security breaches. Increasingly, researchers and practitioners are recognising that information security is not merely a technical issue, but is heavily influenced by social and cultural factors. This paper argues that post-cognitivist approaches to human computer interaction, which focus on situated reasoning and the contextual, relational aspects of computer-mediated activities and interactions, provide a promising set of concepts with which to explore non-technical users' everyday security practices and beliefs. We review the limited research that has been conducted in this area, focussing on the relationship between security and users' more immediate 'real' work, and their perceptions on risk, and show how it is compatible with post-cognitivist understandings. We conclude by outlining some further areas for research.

Keywords
Learning organisation, Knowledge protection, Knowledge management discourse, Tacit knowledge, Organisational knowledge

Disciplines
Business | Social and Behavioral Sciences

Publication Details
This conference paper was originally published as Garrety, K and Barrett, M, Information and computer technology security: furthering the research agenda, ANZAM, Sydney, 4-7 December, 2007.

Information and computer technology security: Furthering the research agenda

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

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

Preferred Stream: Stream 6: Knowledge Management and Intellectual Capital.

Profile: Dr Karin Garrety is a Senior Lecturer in the School of Management and Marketing. She has a PhD in Science and Technology Studies from the University of NSW, and has published in *Social Studies of Science*, *Science, Technology & Human Values* and *Technology Analysis & Strategic Management,* as well as in management journals such as *Human Relations*, *Organization* and the *Asia Pacific Journal of Human Resources.* She is interested in discourse analysis, organisational identity and control, and the politics and management of technology.

INFORMATION AND COMPUTER TECHNOLOGY SECURITY:
FURTHERING THE RESEARCH AGENDA

ABSTRACT: Despite the development of advanced technical devices and procedures, the information held in computer systems remains vulnerable to attack and/or inadvertent mishandling, resulting in security breaches. Increasingly, researchers and practitioners are recognising that information security is not merely a technical issue, but is heavily influenced by social and cultural factors. This paper argues that post-cognitivist approaches to human computer interaction, which focus on situated reasoning and the contextual, relational aspects of computer-mediated activities and interactions, provide a promising set of concepts with which to explore non-technical users' everyday security practices and beliefs. We review the limited research that has been conducted in this area, focussing on the relationship between security and users' more immediate 'real' work, and their perceptions on risk, and show how it is compatible with post-cognitivist understandings. We conclude by outlining some further areas for research.

Keywords: Learning organisation, Knowledge protection, Knowledge management discourse, Tacit knowledge, Organisational knowledge,

Computers and the internet have had a tremendous impact on the way we store, exchange and use information. Many organisations are now almost completely dependent on functioning information systems in order to carry out their tasks. As dependence on these systems grows, however, so too do the threats posed by malicious elements that seek to compromise or destroy the reliability, confidentiality and availability of information held on systems. Security and privacy risks created from inadvertent mishandling of data are no less significant. Mindful of these threats, ICT experts have devised a plethora of technical devices and procedures for the protection 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 technological mechanisms and procedures for establishing and maintaining the security of information, we would expect information in most organisations to be adequately protected from attack and misuse. However, this is not the case. Many ICT specialists have pointed out that information systems are, in general, much less secure than they could or should be, and that security breaches are increasing rather than decreasing in frequency (Lampson 2004; Pahnila, Siponen, and Mahmood 2007; Straub and Welke 1998). To explain this apparent paradox, ICT experts and researchers interested in security problems are increasingly looking beyond the technical aspects of systems. There is growing realisation that future improvements in information security will depend not so much on sophisticated technologies as on a better understanding of the human and social factors that influence the way ordinary users manage security (or fail to) as they work (Fisk 2002; Gonzalez and Sawicka 2002).

In this paper, we draw on insights from 'post-cognitivist' (Kaptelinin and Nardi 2003) understandings of human-computer interaction (HCI) to explore the prospects and problems facing researchers and IT practitioners attempting to understand and improve the practices through which information security is

(or isn't) established and maintained. HCI — in its cognitivist and post-cognitivist forms — has rarely been applied to information security (Adams and Sasse 1999; Besnard and Arief 2004; Gonzalez and Sawicka 2002). The post-cognitivist form, which broadly investigates 'how the use of technology emerges in social, cultural and organizational contexts' (Kaptelinin and Nardi 2003: 692) , is a promising avenue through which to theorise and explore the contextual factors that impinge on information security, and to draw out some salient differences between practices specifically relating to security and other activities for which people use computers.

The paper proceeds as follows. First, we describe same of the more cogent insights advanced by post-cognitivist HCI researchers, particularly those interested in activity theory. Second, we draw on this literature to explore security actions and activities from the 'ordinary' (that is, non-technically specialised) user's point of view. We focus on two issues – the relationship between security practices and normal, 'real' work involving computers, and users' perceptions of risks to the security of the systems they use. Finally, we suggest some new research directions derived from our analysis.

HCI AND ITS POST-COGNITIVIST DEVELOPMENTS

For decades, computer scientists have found it useful and interesting to investigate how humans react to and use computers. Traditionally, these studies drew inspiration, concepts and methods from cognitive science. As a result, they emphasised perception, information processing, memory, attention, and the design of effective computer interfaces (Carroll 2002). Although this approach has been productive and influential, it has also been heavily criticised. As it depends largely on artificial laboratory-based experiments, critics argue that the phenomena and interactions it studies are stripped of the contexts which, in the 'real' world, give computer use its meanings and purposes. Without an appreciation of the social, cultural and organisational contexts in which people use computers, any attempt to theorise human-computer interactions will inevitably remain limited and partial (Bannon 2000; Kuutti 1997).

Since the late 1980s, several related strands of research and theorising in HCI have attempted to address these shortcomings. Taking their inspiration from a range of sources, including hermeneutics, phenomenology, ethnomethodology and speech act theory (Kaptelinin and Nardi 2003), writers working under the umbrella of post-cognitivist HCI have attempted to develop comprehensive understandings of computer use in context. A number of similar but distinct approaches have been developed, including activity theory (Engström 2000; Nardi 1997), computer-supported cooperative work (Bowker, Star, Turner, and Gasser 1997) ethnographic studies of situated computer-mediated actions (Dourish, Grinter, Flor, and Joseph 2004; Suchman 1987) and distributed cognition (Hutchins 1995). For the purposes of this paper, we outline some of the major areas of agreement among these

approaches that are relevant to the issue of information security. Some areas of divergence will also be discussed and highlighted, as they present interesting research challenges for the application of this overall approach to the problem.

Post-cognitivist approaches to HCI are held together by a strong interest in the 'real-life practice of people situated in social and cultural contexts' (Kaptelinin and Nardi 2003: 692). Researchers in this tradition are primarily interested in what people *do* with and through computers, rather than how they process information. Cognition is still relevant, but only insofar as it is part of the on-going flow of activity (Winograd and Flores 1986). Cognition creates meanings, but the meanings of tasks, and the artefacts, operations and relationships used to accomplish them, only emerge in the process of carrying them out (Kaptelinin 1997: 56; Winograd and Flores 1986: 70-1). In other words, an appreciation of the context in which computer-mediated activity occurs is vital. As Suchman (1987: 27-8) writes, 'The coherence of situated action is tied in essential ways not to individual predispositions or conventional rules but to local interactions contingent on the actor's particular circumstances'.

The approaches gathered under the umbrella of post-cognitivist HCI all emphasise contingency and emergent action. Consequently, they downplay or eschew the idea that actions are wholly determined by formal, decontextualised and *a priori* 'rules'. However, there are differences in the degree to which the approaches make space for concepts that more or less loosely encapsulate intent, such as goals or plans, or some of the more enduring features of organisational action, such as habits, divisions of labour, routines, and managerial and cultural expectations. Those writing from the 'situated action' perspective, such as Suchman (1987) and Lave (1988), view plans not so much as determinants or guides of action, but as post hoc resources, invoked to explain actions after they have occurred (Suchman 1987: 27. See also Nardi 1997). Activity theory, on the other hand, allows space for intentionality as a motivating force, in the form of 'objects' towards which actions are directed. In this view, 'objects' are one of several elements that make up the overall structure of activities. Subjects (people) pursue objects within contexts comprised of tools, members of the relevant community, divisions of labour, and rules, in the form of 'explicit and implicit norms, conventions and social relations within a community' (Engström 2000; Kuutti 1997: 28). Objects, and the other elements that comprise activities, may change as those activities proceed. Activities are 'longer-term formulations' typically comprising several steps or phases, for example, writing a conference paper. They consist of chains of actions, such as deciding on a topic, gathering references, reading, writing, revising, and so on. At a more fundamental level, actions 'consist of chains of operations, which are well-defined habitual routines used as answers to conditions faced during the performing of the action' (Kuutti 1997: 30-1), such as switching on the computer, using a database, printing and typing. The activity provides the context for the actions and operations.

For the purposes of this paper, activity theory offers some useful concepts through which to examine the activities, actions and operations involved in establishing and maintaining information security. For activities to run smoothly, the various contextual features need to be more or less aligned. Often, and this is particularly relevant to security practices, users experience 'contradictions', or 'problems, ruptures, breakdowns, clashes' that occur when there is 'a misfit within elements, between them, between different activities, or between different developmental phases of a single activity' (Kuutti 1997: 34). An example relating to information security would be the tensions many of us feel when we make decisions about passwords. Do we opt for convenience, using an easily remembered, unchanging password for multiple uses, or do we privilege security, struggling to memorise multiple unwieldy combinations of numbers and letters, which change frequently? Such tensions or 'contradictions,' to use the term more common in activity theory, may provide opportunities for learning and innovation. However, this is not *necessarily* the case. First, tensions or contradictions need to be perceived as such. Second, they have to matter enough to become the objects of a new round of activity, namely, problem solving.

There is some work that has examined information security from the 'ordinary' (non-technically trained) user's point of view. While very little of this work has explicitly examined security tasks in the context of potentially contradictory work pressures and demands, extant findings generally support the claims made above about the perceived tensions between security demands and the pressure of other tasks. However, there is much more work to be done. We now review existing work on information security from the user's point of view in the light of the above discussion, before returning to problems and prospects for further research.

INFORMATION SECURITY FROM THE USER'S PERSEPCTIVE

Information security and 'real' work

Although malicious attacks by external hackers can wreak havoc with an organisation's information systems, many ICT experts believe that insecure actions by employees, characterised by one group of researchers as 'dangerous tinkering' and 'naive mistakes' (Stanton, Stam, Mastrangelo, and Jolton 2005), are largely responsible for breaches, and for leaving companies open to attack from outside (Dinnie 1999; Pahnila et al. 2007). Insecure actions on the part of employees can include poor password practices, failure to update virus protection software, opening dangerous attachments, supplying personal information to 'phishers', and leaving 'logged on' computers unattended (Besnard and Arief 2004; Dourish et al. 2004; Gross and Rosson 2007).

Despite the apparent prevalence of these insecure actions, empirical research into users' attitudes has found that they often do profess an awareness of security. The problem is that the *practice* of security is hedged about with uncertainties and compromises (Adams and Sasse 1999; Dourish et al. 2004; Gross and Rosson 2007). Clearly, there is much more to the establishment and maintenance of security than an awareness of its importance. Secure and insecure *actions and operations*, and their relationships to 'knowledge' and 'awareness', need to be examined in the overall context of computer-mediated activities. This as an area of HCI that is seriously under-researched. In a recent paper, Gross and Rosson (2007) went so far as to claim that 'no work has yet investigated why user action and belief are inconsistent'. While there has indeed been very little deliberate and systematic research along these lines, enough is known about the nature of computer-mediated work and risk perceptions to enable some speculation.

People at work use information technology to accomplish tasks, for example, the creation and maintenance of databases, the writing of reports, communication with colleagues, and research. These activities and actions constitute the 'real' work of employees, the tasks that occupy most of their time and attention. They are pursued within contexts containing technologies, colleagues, divisions of labour and formal and informal rules that guide the action. Jobs are rendered doable by aligning these contextual factors in ways that support getting the 'real' work done, that is, achieving the salient objects. If we conceptualise work this way, we can appreciate how and why the establishment and maintenance of information security can become problematic. In pursuing the 'real' work, security measures can be experienced as obstructions or contradictions. Adams and Sasse (1999: 43) found this to be the case when they surveyed and interviewed users about passwords: 'Users [...] perceive many security mechanisms as laborious and unnecessary – an overhead that gets in the way of their real work'. Dourish et al. (2004: 394) reported similar findings, particularly among their younger, more technologically experienced interview subjects: 'They were more likely to talk about security in terms of its costs as well as its benefits, and frame technical security measures as ones that can interfere with the practical accomplishment of work'.

Employees engaged in 'real' work often have fairly clear ideas about what the object(s) of the activity is/are, how the tools work, and where their responsibilities lie. Security work is much more nebulous. As Gross and Rosson (2007) point out 'end-user security management is not task-oriented – it lacks the specific goals, resources, boundaries, and constraints that mark tasks'. Although it encapsulates a 'high-level objective' (2007:2), it is not as goal-oriented or as time-bounded as many 'normal' work tasks. There is no beginning or end to security work, and users receive little feedback concerning their efforts, or lack of efforts. The outcome of the work – the end-result – is not clear. Also, as many organisations employ specialised ICT staff, non-ICT employees are aware of a division of labour regarding ICT tasks. However, because security is not a core task for them, they are unclear as to

where their own responsibilities lie, relative to those of the ICT personnel. Users often delegate responsibility for security to the ICT staff (Dourish et al. 2004; Foltz and Hauser 2005; Gross and Rosson 2007). The non-core nature of security work, coupled with the opportunity of shifting responsibility to the ICT staff, helps explain why users tend not to be very knowledgeable about security threats and the mechanisms devised to prevent them. General awareness is there, but detailed knowledge is often lacking (Dourish et al. 2004; Foltz and Hauser 2005; Gross and Rosson 2007). From the perspective of post-cognitivist HCI, this is precisely what we would expect. People pursue and acquire knowledge within the contexts of the activities that are meaningful to them. If users perceive security as peripheral, annoying or someone else's problem, they will hardly be motivated to inform themselves about it (Fisk 2002).

Users' attitudes to security and their engagements with it are clearly complex and sometimes contradictory. Attempts by researchers to investigate the contextual factors that impinge on users' practices and beliefs about security fall into different categories. First, there are theoretical models that try to bring the various factors together, and explore relationships among them. In some cases, these form the basis for surveys and statistical analyses (Gonzalez and Sawicka 2002; Kotulic and Clark 2004; Pahnila et al. 2007; Woon and Pee 2004). For example, Pahnila et al. (2007) found that while sanctions and rewards have little impact on the practice of securiety, 'attitudes, normative beliefs and habits have [a] significant effect on intention to comply with IS security policies'. While these studies are useful for establishing statistical correlations among variables in the populations studied, they cannot capture the rich textures of compromise, confusion and creativity that become evident when the research methods employed are more open-ended and qualitative.

Such studies of user practices and perceptions are rare. Dourish et al. (2004) conducted interviews with 20 employees in two organisations. The employees in their sample managed security in unexpected ways that were often technically simple, but effective. For example, they deliberately used vague language, such as 'I took the actions you requested', in emails containing sensitive information, as this was much easier than using encryption tools. They also 'switched media', that is, used the telephone or spoke face-to-face to convey sensitive information (2004:397). They arranged their offices so that computer screens faced away from prying eyes. In other words, security practices were not confined to on-line technologies, but managed more holistically within the physical work space with its multiple tools and relationships. Another manifestation of users' tendency to view 'security' in holistic terms was their disinterest in making the same sorts of distinctions that IT experts do. For example, spam, viruses and passwords sniffers were lumped together as problems, and solutions, such as firewalls, were perceived to be effective against all possible threats (2004:394).

Gross and Rosson (2007) reported similar findings from their interviews with 12 users from a range of different organisations. These users were aware of the sensitivity of the information they handled, and took measures, sometimes physical (locking rooms and computers), to keep it secure. The majority reported taking care with passwords, and being suspicious of email requests for personal details ('phishing'). Again, however, most were unclear about the technical details of security threats and protective devices. They confused viruses with worms, and were unsure about their computers' virus protection capacities. In another example of ordinary users' tendency to view security holistically, interview subjects in this sample tended to conflate security with functionality. In discussing threats, many did not distinguish between external attacks or internal software faults. Such distinctions were of little or no relevance compared to the main items of interest – the functionality of the computer and the availability of data.

We can, therefore, perceive security work as a potentially contradictory element within overlapping structures of activity. Users perform security-related actions in the course of their 'real' work, but the tools used to perform them are often mystifying, and the actions themselves can delay, complicate and obstruct the main line of activity. Users often try to resolve contradictions by ignoring, downplaying or circumventing those aspects of security that they perceive as too intrusive or technically confusing. They sometimes devise their own, more comprehensible modes of dealing with sensitive information, and frequently delegate the technical details of information security to others who are perceived to be more knowledge than they are.

Perceptions of risk

In this section of the paper we focus on the uncertainties surrounding the *object* of security activities. An intangible or tangible object, such as 'security' or 'a secure system', provides a unifying motive and rationale for those engaged in a particular activity. It is the 'something' that differentiates one set of actions and operations from another, a 'something' that can be jointly manipulated and transformed by those who participate in it (Kuutti 1997: 27). However, as we saw above, many end-users participate only reluctantly, uncertainly or sporadically in security activities, as their priorities and areas of expertise lie elsewhere. How do users view security as an object? To answer this question, we need to consider the concept of risk, as it is the perception and prevention of risk that gives security activities their meaning and purpose. As Dourish and Anderson note, 'formulations of privacy and security must, implicitly or explicitly, draw on or respond to models of risk and danger' (2006: 322).

Many writers in the field of information security, under the influence of cognitivist theories of information processing, assume that users are rational actors who, once informed of the 'objective' threats to security, will adjust their behaviour accordingly (Dourish and Anderson 2006: 325-7).

Increasingly, however, theorists in information technology, as well as across a range of disciplines, including sociology, psychology and economics, are abandoning the notion that people perceive and respond to risks in ways that reflect 'objective' expert assessments of the dangers that exist 'out there'. Instead, assessments of risk are influenced by emotions, the way information is presented, the perceived proximity in time and space of the perceived threats, and particularly the cultural and social meanings of the putative threats within the individual's community (Dourish and Anderson 2006; Taylor-Gooby and Zinn 2006).

Work that has examined users' perceptions of information security risks confirms this latter view. In a large survey of the Swedish general public, Sjöberg and Fromm (2001) found that users were generally well-disposed towards information technology. They rated 'IT risks', which included virus infection, invasions of privacy and credit card fraud as 'quite small when considered as personal risks, but quite sizable when considered as risks for others' (433). The authors of the study found this quite interesting, as lay people generally overestimate risks to themselves from new technologies, and see themselves and others as more or less equally susceptible to danger. To account for these unusual findings, Sjöberg and Fromm suggested that because users 'are actually operating the technology, something that never happens in cases such as nuclear power', they feel a sense of familiarity and control (438). Relatively few had experienced security problems -- 3.5% had been infected with a virus via the internet, 3.9% by virus via email, 0.6% experienced credit card fraud, and 1.3% privacy intrusion (434). Sizable segments of the survey population reported taking preventive actions against these, such as using antivirus programs (41.1%) and aliases (7.6%) or refusing to use credit cards on the internet (51.8%). Given these numbers, it is not surprising that users perceived themselves, from their personal experience, to be at relatively low risk and in control of keeping risks at bay. For some commentators on information security, lay perceptions such as these, which are based on personal experience, are deeply problematic. They are evidence that users 'lack knowledge'. For example, Adams and Sasse (1999) wrote 'users are not sufficiently informed about security issues. This causes them to construct their own model of possible security threats and the importance of security and these are often wildly inaccurate. *Users tend to be guided by what they actually see – or don't*' (43, emphasis added).

The relationship between perceptions of risk based on what users actually experience and their more general beliefs about the dangers that lurk 'out there' in cyber space is particularly interesting. In the Swedish study just cited, personal experiences contributed to a downplaying of threat to the self. However, the broader threats were still recognised quite strongly, in the form of perceived risks to others. In their interview-based study of security practices in two U. S. companies, Dourish et al. (2004) provide some additional insights into how users perceive these more distant and less controllable sources of risk. Among their subjects, they found 'an overwhelming sense of futility'

regarding hackers and stalkers who, they thought, would 'always be one step ahead'. These perceptions created frustration, and a 'fictive norm of adequate protection, against which people continually find themselves wanting' (394). In other words, the object of security practices is paradoxical and ultimately elusive. While on a day-to-day basis, we may experience our own computers as relatively safe, particularly if we follow routine precautions, we can never be sure. The killer virus may be just about to attack, and someone may have stolen our identity without our knowledge. Someone out there might have our credit details. The nebulousness and uncertainty surrounding security, particularly the fact that we never really know whether we are secure or not, has significant implications for learning, and for the management of information security in organizations.

CONCLUSION: FURTHERING THE RESEARCH AGENDA

There are many possibilities for research which emerge from these observations and findings. Post-cognitivist HCI, and particularly the concepts and relationships suggested by activity theory, holds promise for improving our understanding of the social and cultural contexts that influence the establishment and maintenance of secure ICT practices. Within this perspective, research can focus on different levels.

Individual level

At an individual level, further work is needed to understand the compromises and the inventiveness of employees in ensuring ICT security. For example, it would be useful to investigate how individual users' simple, non-technical actions and operations interact with broad-based technical tools and actions, and how the users' 'mental models' of security may either compromise or enhance it. It will be particularly important to understand how these mental models play themselves out in situations of conflict or tension arising from other tasks.

Group or community level

In addition, more needs to be known about how different *groups* of users may experience tensions with regard to security practices, and how individuals' perceptions of responsibility for security may be influenced by their membership of a particular community of practice (Wenger 1998). Groups likely to be of interest include expert and non-technically specialised users, but other groups may also be worthy of investigation. For example, we might usefully consider differences in perceptions of responsibility for security between work groups who see themselves as handling sensitive information and those who don't see themselves this way but whose interactions with ICT may still inadvertently or occasionally maliciously expose the organisation to security risk.

Inter-group comparisons

We might also compare groups by asking questions such as: Are there recurring patterns in the types of security tensions experienced by users in various groups? How do groups vary, if at all, in how they manage, if not resolve, these tensions in their day to day work? What contextual factors, including the difference kinds of work performed in particular groups, influence the situated decision-making about perceived conflicts between 'security' aspects and 'real' aspects of tasks? In what work or other contexts are tensions or contradictions absent and does this differ between groups?

From groups to cultures

We might derive new practical questions focussed on improving ICT security, aided by a more sophisticated understanding of how individuals and groups incorporate understandings and practices around security into the context of their work. Influenced by this contextual focus, some changes and extensions to the traditional, technically-focussed research approach suggest themselves. For example: How might understandings of situated learning, for example, learning within communities of practice (Wenger 1998) allow us to see how group 'solutions' to security tensions become entrenched? Beyond this, to what extent do particular groups' 'solutions' – understood as local ways of managing tensions around security and other work demands - become part of an organisation's culture? How might an organisation's security culture(s) be influenced by interventions within the separate communities of practice within the organisation?

Exemplary organisations

As well as studying different approaches to ICT security in organisations in general, it could be valuable to examine the approach to ICT security of organisations which have had an exemplary ICT security record. At first glance this may seem counter-intuitive. After all, the tradition of researching various forms of organisational *failure*, such as studies of the Columbia space shuttle disaster, is well established. This tradition has led to important insights into how aspects of organisational culture may affect specific decisions resulting sometimes in catastrophic error. The assumption is that other organisations can avoid similar errors by studying what went wrong in a particular case.

However this is not the only possible approach or even the most apt for ICT security. It is often pointed out that the nature of ICT attacks changes frequently, typically in the direction of greater sophistication, so that that fixes often lag behind technical understandings of the problem, even in 'expert' environments. Nevertheless over time some organisations, through attention to specific non-

technical as well as technical practices may be shown to have performed better than other, apparently similar organisations at managing achieving the vague, ephemeral goal of better ICT security. Similar questions might be asked of them as need also to be asked about achieving better occupational health and safety records. How do some organisations manage to fend off or be immune to a particularly pervasive virus when others succumb? What were the users in the unscathed organisation doing or thinking differently? How might these thought processes be transferred to less well performing organisations?

Insights from team research

Finally, it may make sense to apply insights from areas of knowledge which link individual and group-based work via teams. An example is Katzenbach and Smith's (1993) analysis of the problems and advantages of different kinds of team structures. These researchers found that, although all teams have some common needs, specific team structures impose some special requirements for the team to function effectively. For example, 'assembly line' teams have to deal with the fact that their work does not naturally throw up markers of progress and achievement. Such teams need to invent and interpose their own performance measurements so that members can inform themselves of the team's achievements and celebrate them appropriately. The endless, ephemeral 'no news is good news' nature of much ICT security work suggests a parallel with this type of team. Research could thus focus on how to manage the ICT security work process to impose achievement markers – beacons in the nebulous security landscape.

These research approaches incorporate an awareness that ICT security risks often appear both far away and trivial so it is difficult for people to maintain a sense of urgency about them. At the same time the tools for ensuring security often appear unfamiliar and mystifying, and yet unimportant for non-technically specialised users. Combining this with an unclear division of labour and mental models which may be wildly inaccurate add to the zones of uncertainty around ICT security. The research agenda set out here suggests that context-based research into how users actually think about, devise, reject, employ, and improvise work routines affecting computer security will be vital for understanding and reducing these zones of uncertainty.

REFERENCES

Adams, A, and Sasse, M A (1999). Users are not the enemy. *Communications of the ACM, 42*(12): 41-46.

Bannon, L J (2000). Situating workplace studies within the human-computer interaction field. In P Luff, J Hindmarsh and C Heath (Eds.), *Workplace studies. recovering work practice and informing systems design* pp. 230-241. Cambridge: Cambridge University Press.

Besnard, D, and Arief, B (2004). Computer security impaired by legitimate users. *Computers & Security, 23*: 253-264.

Bowker, G C, Star, S L, Turner, W, and Gasser, L (Eds.). (1997). *Social Science, Technical Systems, and Cooperative Work. Beyond the Great Divide*. Mahwah, New Jersey: Lawrence Erlbaum Associates.

Carroll, J M (2002). Introduction: Human-computer interaction, the past and present. In J M Carroll (Ed.), *Human-computer interaction in the new millenium* pp. xxvii-xxxvii. New York: ACM Press.

Dinnie, G (1999). The second annual global information security survey. *Information management and Computer Security, 7*(3): 112-120.

Dourish, P, and Anderson, K (2006). Collective information practice: exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction, 21*: 319-342.

Dourish, P, Grinter, R E, Flor, J D d l, and Joseph, M (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing, 8*: 391-401.

Engström, Y (2000). Activity theory as a framework for analyzing and redesigning work. *Ergonomics, 43*(7): 960-974.

Fisk, M (2002). *Causes and remedies for social acceptance of network insecurity.* Paper presented at the Workshop on Economics and Internet Insecurity.

Foltz, B, and Hauser, R (2005). *Faculty awareness of university computer usage regulations.* Paper presented at the 2005 Southern Association of Information Systems.

Gonzalez, J J, and Sawicka, A (2002). *A framework for human factors in information security.* Paper presented at the WSEAS International conference on information security, Rio de Janiero.

Gross, J B, and Rosson, M B (2007, March 30 - 31). *Looking for trouble: Understanding end-user security management.* Paper presented at the Proceedings of the 2007 Symposium on Computer Human interaction for the Management of information Technology Cambridge, Massachusetts.

Hutchins, E (1995). How a cockpit remembers its speeds. *Cognitive Science, 19*: 265-288.

Kaptelinin, V (1997). Computer-mediated activity: Functional organs in social and developmental contexts. In B A Nardi (Ed.), *Context and consciousness. Activity theory and human-computer interaction* pp. 45-68. Cambridge Massachusetts: MIT Press.

Kaptelinin, V, and Nardi, B (2003). *Post-cognitivist HCI: Second wave theories.* Paper presented at the CHI 2003: New horizons, Ft Lauderdale, Florida, USA.

Katzenbach, J R, and Smith, D K (1993). *The wisdom of teams : creating the high-performance organization*. Boston, Mass: Harvard Business School Press.

Kotulic, A G, and Clark, J G (2004). Why there aren't more information security research studies. *Information & Management, 41*(5): 597-607.

Kuutti, K (1997). Activity theory as a potential framework for human-computer interaction research. In B A Nardi (Ed.), *Context and consciousness. Activity theory and human-computer interaction* pp. 17-44. Cambridge Massachusetts: MIT Press.

Lampson, B W (2004). Computer Security in the Real World. *Computer, June*: 37-46.

Lave, J (1988). *Cognition in practice : mind, mathematics, and culture in everyday life*. Cambridge: Cambridge University Press.

Nardi, B A (1997). Activity theory and human-computer interaction. In B A Nardi (Ed.), *Context and consciousness. Activity theory and human-computer interaction* pp. 7-16. Cambridge Massachusetts: MIT Press.

Pahnila, S, Siponen, M, and Mahmood, A (2007). *Employees' behavior towards IS policy compliance.* Paper presented at the 40th Annual Hawaii Conference on System Sciences, Hawaii.

Siponen, M 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.

Stanton, J M, Stam, K R, Mastrangelo, P, and Jolton, J (2005). Analysis of end user security behaviors. *Computers & Security, 24* (2): 124-133.

Straub, D W, and Welke, R J (1998). Coping with systems risk: security planning models for management decision-making. *MIS Quarterly, 22*(4): 441-469.

Suchman, L A (1987). *Plans and Situated Actions. The Problem of Human-Machine Communication*. Cambridge: Cambridge University Press.

Taylor-Gooby, P, and Zinn, J O (2006). Current directions in risk research: New developments in psychology and sociology. *Risk Analysis, 26*(2): 397-411.

Wenger, E (1998). *Communities of Practice*. Cambridge: Cambridge University Press.

Winograd, T, and Flores, F (1986). *Understanding computers and cognition: A new foundation for design*. Norwood, New Jersey: Ablex Publishing Company.

Woon, I W Y, and Pee, L G (2004). *Behavioral factors affecting internet abuse in the workplace - an empirical investigation.* Paper presented at the Third annual workshop on HCI research in MIS, Washington DC.