Human and Organizational Issues for Resilient Communications

Tom Anderson, Jeremy Busby, Antonios Gouglidis, Karen Hough,
David Hutchison and Mark Rouncefield

Abstract Human and organizational issues are able to create both vulnerabilities and resilience to threats. In this chapter, we investigate human and organizational factors, conducted through ethnographic studies of operators and sets of interviews with staff responsible for security, reliability and quality in two different organizations, which own and operate utility networks. Ethnography is a qualitative orientation to research that emphasizes the detailed observation and interview of people in naturally occurring settings. Our findings indicate that 'human error' forms the biggest threat to cyber-security and that there is a need for Security Operational Centres to document all cyber-security accidents. Also, we conclude that it will always be insufficient to assess mental security models in terms of their technical correctness, as it is sometimes more important to know how well they represent prevailing social issues and requirements. As a practical recommendation from this work, we

Tom Anderson
School of Computing and Communications, Lancaster University, LA1 4WA, UK,
e-mail: t.anderson1@lancaster.ac.uk

Jeremy Busby
Management School, Lancaster University, LA1 4YX, UK,
e-mail: j.s.busby@lancaster.ac.uk

Antonios Gouglidis
School of Computing and Communications, Lancaster University, LA1 4WA, UK,
e-mail: a.gouglidis@lancaster.ac.uk

Karen Hough
School of Computing and Communications, Lancaster University, LA1 4WA, UK,
e-mail: karenhough1@hotmail.com

David Hutchison
School of Computing and Communications, Lancaster University, LA1 4WA, UK,
e-mail: d.hutchison@lancaster.ac.uk

Mark Rouncefield
School of Computing and Communications, Lancaster University, LA1 4WA, UK,
e-mail: m.rouncefield@lancaster.ac.uk

suggest that utility organizations engage in penetration testing and perhaps other forms of vulnerability analysis, not only to discover specific vulnerabilities but also to learn more about the mental models they use.

1 Introduction

Communication networks are increasingly seen as critical infrastructures, and their resilience – the ability to offer an acceptable level of service despite the challenges that threaten them – is the subject of this book [10, 21, 22]. In this chapter, we report on the often neglected but crucial human and organizational issues in communication networks resilience. Networked systems are generally complex, and they have three aspects that need to be considered in combination when building resilience into them: these are technology, organization, and people, as illustrated in Fig. 1. The approach we take is to study utility networks, which are examples of cyber-physical systems that offer a suitably general model for our work [4, 6].

A common approach towards conceptually understanding cyber-physical systems is to divide them into 'levels', based on their function. Devices, boundaries, processes, etc. are then associated with each level, depending on the industry and network topology in question. Nevertheless, in all cases, there is a clear indication of the complexity and interconnections between the levels. To cope with the different levels and for achieving resilient communications we propose the investigation of systems based on three viewpoints, viz. *Organization*, *Technology* and *Individual* (OTI) [5].

The application of the OTI viewpoints, depicted in Fig. 2, enables a broader view of the system, i.e., a representation of the whole system from the perspective of a related set of concerns. Thus, this helps to increase the level of threat awareness by

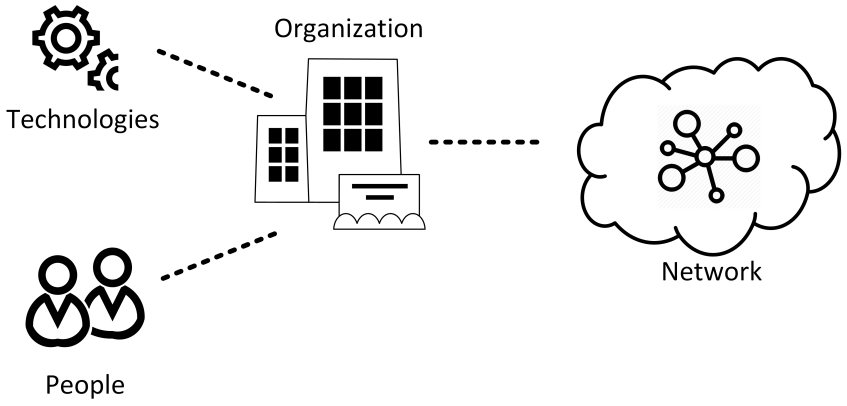

Fig. 1 Technology, organization, and people in networked systems

identifying potential vulnerability-creating behaviours. Specifically, the three viewpoints are concerned with: *The organization viewpoint*, with the groups of people who work together in an organized way for a shared purpose as well as any policies, processes and procedures in the organization; *The technology viewpoint*, with the implemented technologies in a system including the software, hardware and network components, as well as any communications among them; *The individual viewpoint*, with the way a single person or entity acts or behaves in a specific situation or under particular conditions.

OTI can be used to increase awareness on both technical and non-technical risks. The technical risks may be identified by conducting several security assessments [12]. These may unveil potential vulnerabilities and also provide information on how they can be exploited. However, such activities may not be able to provide enough context on human and organizational aspects. When the latter is combined with technical findings, it may lead to the construction of more resilient strategies against cyber-attacks. The investigation of human and organization may help to successfully identify people and their roles; understand the policies used in an organization; identify social relations among employees; understand their behaviour, etc. That information may refine the input required by OTI and risk management approaches [16, 17] and help to define preventive processes in the sense of estimating and minimizing the risk of successful cyber-attacks (e.g., ransomware [13], advanced persistent threats [7]).

The investigation of organizational factors in utility organizations includes two ethnographic studies of operator practices in different utilities, especially their use of mobile devices but more widely the vulnerabilities that arise from working conditions, technology affordances and social context. For us, issues of resilience and security are not simply, or merely, technical issues resolved by technical means. Instead, we see the prevalence of what are termed 'human factors' – and especially when it comes to failures of various kinds. Accordingly, we would like to say a little

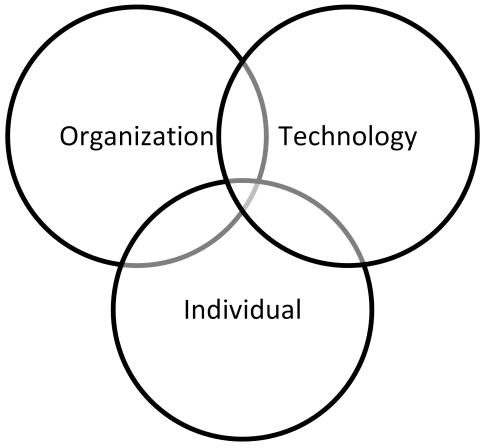

Fig. 2 The OTI viewpoints

about the ethnographic stance we have adopted to the research. Ethnography is a qualitative orientation to research that emphasizes the detailed observation and interview of people in naturally occurring settings – in this case two utility companies. The main virtue of this ethnographic approach lies in its ability to make visible the 'real world' sociality of a setting – to tell us something about what working in that environment is actually like – to unpack some of the 'human factors' involved – or in this case what the security concerns of those working in any particular domain might look like. The emphasis then is on producing reasonably detailed descriptions of the everyday 'workaday' activities of social actors who live and work within the setting, developing an 'appreciative stance' of the nature of the work and the perceptions of those involved. The concern is to get some kind of access to the everyday ways in which participants understand and conduct their working lives, in this case, their understanding and perceptions about various kinds of cyber-risk and vulnerabilities.

2 Ethnographic Research

The aim of our ethnographic work was to assemble some account of the different ways in which people, as organizational actors, managed and organized their everyday working lives, with a particular emphasis on everyday security. This necessitates the fieldworker becoming involved in some sense in the setting itself and the everyday activities being carried out. It requires some willingness to pay full attention to what people are doing and what people are saying, in order to gain the same perspective, as far as this is possible, of the actors concerned; and counteracting the temptation, when studying others' lives, to read things into them. The aim was to observe, record and describe the phenomena of everyday organizational life independently of any existing theories and methods. This involves dispensing with conventional research preconceptions that there are numerous things that people are doing that are trivial, the mere fact that people are doing them justifies the attention given by the researcher. We are resolutely interested in our participants. What kinds of things do they take for granted or presuppose in going about their work, what kinds of things do they routinely notice, what kinds of things are they on the lookout for? How do they tune themselves in to the state of being at work?, what are the constituents of their 'serious' or 'at work' frame of mind? How do they react to the things that occur within their sphere of attention?, what objectives are they seeking to attain in their reactions to whatever occurs? (see Table 1).

The observations and the ethnographic interviews were concerned with some general questions on experience and perceptions of security and risk, as well as with any working 'model' of risk held by our participants.

So, for example, we asked questions concerning:

1. What do they perceive as risky, and why? What do they perceive as NOT risky and why? Does this change, has it changed, will it change?

Table 1 Precepts for ethnographic analysis

Precepts
1. Assume that the world is socially organized – and show how this orderliness is accomplished.
2. See the setting and its activities as socially organized from within.
3. Understand the setting and its activities in terms that members understand.
4. Examine activities in all their detail.
5. Treat activities as situated – activities are not isolated but situated within a context.
6. Attend to the 'working division of labour' – understand coordination.
7. Tasks and activities are sequenced – integral to the interactional sense of activity.
8. Attend to the egological organization of activities – people do things not organizations.
9. Do not draw a distinction between expert knowledge and practical knowledge.
10. Do not treat settings as equivalent – beware spurious and unwarranted generalization.

2. How is their view different from other people? How is it the same? Are there incongruences, contradictions within one informant or between different informants?

And in our analysis we were interested in:

1. Models of Risk: How did each of the interviewees model risk?
2. How did the different models of risk play out with each other? Were there co-existing models within the same person?
3. How did the models of risk change?

Our ethnographic studies were conducted on the premises of two different organizations, including an information service provider (ISP) and a utility provider, both located in the European Union. The participants were initially provided with a consent form, which provided information about the nature of the project, the procedures of our studies and their rights under the data protection act. A diverse group of people were interviewed in both organizations, including security administrators/analysts/engineers, managers, customers support personnel and technicians. The research findings of our analyses are presented in the following section.

3 Research findings

Below we present some very brief and anonymized (and perhaps, therefore, relatively anodyne) excerpts from the research, primarily to give some general indications of the approach and our initial findings, and presented so as to preserve confidentiality and our participants' anonymity. Since this chapter is in the public domain we have made judicious selections from the more comprehensive fieldwork reports that were made available to the project members.

Firstly, in our information service provider, in terms of procedures for notification and response to a security incident; staff were alerted directly by emails or SMS, or

by other junior staff, of any cyber-security incidents. However, all of the staff interviewed had problems giving precise details regarding the exact protocols to follow. They stated that often to save time, nobody looked for the origins of the security incident but only at how to remedy it. There also seemed to be some confusion among them regarding the exact procedures and most limited themselves to talking about prevention, i.e., administrating back-ups and anti-virus updates. In terms of the controls adopted; they were deemed to be of both a social and technical nature. Most of those interviewed talked about the strict controls put in place regarding physical entry to data sensitive areas, including most notably the data centre. Access was limited to just 20 people and special badges and fingerprinting controls were in place.

Reported security incidents were variously categorized as: a) human error – such as responding to a spam email; b) training failures – this included issues of the physical security of buildings as well as failure to up-date virus software and firewalls; and c) outside hackers, since many of those interviewed mentioned the threat of malware attacks on data and master boot records rendering systems inoperable. Interestingly the main threat to security however was deemed to be accidental rather than malicious.

In terms of solutions proposed by the staff: our researcher was clearly told that more investment was needed. Many suggested that one solution needed was to encrypt all the hard discs of all computers. All of the staff interviewed stated that they wanted to install real time surveillance software including intrusion detection systems (IPS), intrusion prevention systems (IPS) and one employee suggested using a military type device lock apparatus to prevent data loss. Most suggested that they should focus on prevention more than anything i.e., back-up of data and keeping anti-virus software up to date. Improving security, they said, was held back by a lack of funding and lack of acknowledgement of real threats; as one person stated, 'it is important that it works, not that it is the best', and 'when it doesn't work anymore they simply want to plug the hole and not pay too much to buy new software. We have many problems due to old obsolete machinery that is not compatible with new technology'.

There was also more focus placed on physical security i.e., securing the premises with fences and closed-circuit cameras and infrared structures (as they have found thieves on the premises) than on cyber-security. Some staff stated that security often came down to the individual conscience, what they personally felt was right. However, the overall consensus was that the most successful intervention to improve cyber-security would be to create rigorous training courses for all staff at all levels. There was an impression that many training courses in cyber-security were undertaken to fulfil legal obligations and were not necessarily taken seriously by staff. In terms of a 'Bring Your Own Device (BYOD) Policy': since a BYOD policy can present a number of potential security risks, the company provides the devices (so there is no BYOD) and depending on their particular job each individual could choose which brand since all acquisitions were usually related to job needs. A cyber-security incident was reported that happened in the control room due to an infected pen drive being inserted into a computer by an external consultant. The incident

was deemed to be an 'accident' as the person was 'well known' and 'trusted' and 'a good person'. The impact of this event in terms of downtime was variously reported as participants were genuinely worried about reporting negative things, 'we do not spit on the plate from which we eat'. Employees were allowed to take their personal telephones on site, although they were not permitted to use them in certain areas. The participants themselves did not perceive smart-phones as posing any risk to cyber-security since they were never used to connect to the networks. One participant stated that the most one could do was 'take a photo of the control room and monitors and maybe sell it to an interested party' – suggesting a lack of knowledge of some of the security implications of smart-phones. Some employees had copies of non-standard software on their computers. The reason they downloaded this software was because it was deemed essential for their job, but the company did not have the resources to buy it. In conclusion, for this organization (but perhaps reflecting the circumstances of many other organizations), we can state that there appeared to be an overall consensus in identifying human error as the biggest threat to cyber-security. Many said that there needed to be a change in culture in which staff at all levels were made to realize the importance of cyber-security and appropriate training. The main technical improvements to cyber-security nominated by staff were those of real time surveillance software, such as IPS, IDS, NAC (network access control) systems. Another important finding was that staff themselves complained about the lack of centralization regarding cyber-security issues. The need for a Security Operational Centre that documented all cyber-security incidents was deemed fundamental by the staff; in particular it was considered essential for controlling the security centrally on site. One respondent stated that, "each person is responsible for looking after their own garden" meaning that the system is fragmentary and that the different companies working together at the site all took care of their own sector and that there was no coordination between them. In Table 2, we summarize the identified issues, incidents and solutions in the information service provider organization.

Second, in our utility provider, we again provide some (anonymized) extracts and quotes from the interviews concerning cyber-security with various staff at the utility

Table 2 Resilience: Information service provider

	Information service provider
Issues	Procedures for notification and response. Controls adopted; social and technical nature. Security - lack of funding and lack of acknowledgement of real threats. Lack of centralization regarding cyber-security issues.
Incidents	Security incidents categorized a) human error; b) training failures; c) external hackers. Human error - biggest threat to cyber-security.
Solutions	Investment; encryption; real time surveillance software; rigorous training courses. Focus on prevention; focus on physical security.

provider. One interviewee perceived the company's risk as low, explaining that some security systems are currently deployed, but that security is not a priority at the moment. Cyber-attacks were not seen as probable, and, consequently, as very low risk. The other risk the interviewee was most conscious of was the Wi-Fi. This is most evident because of the fact that they believe that equipment they normally use has a propensity to get viruses. Also, their devices (e.g., both their personal and work ones) can connect to the Wi-Fi directly at work, without much in terms of controls. But, even so, the interviewee did not regard this as being too risky: it was suggested that their level of risk was like any other company that had a clients' database; and because when someone, such as a hacker, enters the Wi-Fi, he/she can, for example, command a concentrator to stop, but nothing much else, in the way of malicious operations can be done. They suggested that therefore there was little value or reward to any hacker who hacked the system. Consequently, the interviewee regarded usability as more important than prevention because they did not really feel they were under risk. However, the tools that prevent security intrusions also sometimes reduce usability and both the company and the employees seemed to prioritize usability over protection/security. This kind of prioritization is done, and is seen, for example, in enabling employees to connect from home and see a customers' data, in case a customer rang with a query or even to re-establish power if power had been cut. However, they argued that having in place a range of security mechanisms not permit performing such operations could risk customer displeasure.

For another interviewee, the risks of intervening using 'informatics' also seemed very low. Specifically, they seemed not to be worried about Internet security risks because many of the same things (security breaches), that might be achieved through the Internet, could be done through other means. The only possibility they saw was where somebody controlled the Smart Meter (SM) (counting less, counting more, bringing it down to zero). This is a case where they acknowledge the existence of a risk. Yet, it was not considered to be important for someone to be able just to read a SM. Something that could be done is to change the meter reading, but electronic tricks in that sense are unheard of. This is something they said could be done mechanically or manually on the SM; however, they have not yet seen this done by means of IT'. Furthermore, it is believed that the level of security they have is the appropriate one. Despite the fact they state that their assets are not very desirable, they also indicate that more IT-based security could be put in place.

In terms of cascade effects and interdependencies, it was mentioned that if there was no power, the Internet can not work because of its interdependency with electricity distribution. Looking at other, related, interdependencies, the police force was mentioned as a service that might thereby be impacted by malicious intrusions. If there is no power or phone and there is an emergency, the police would not be in position to find it out or respond. This means that somebody could intrude into their system and disturb such services. Therefore, a possible impact on their communication services was identified as being among the most important ones. Furthermore, it was said that in the absence of an Internet connection, a reading of a SM would be infeasible. However, this was not believed to be a problem since this is an operation that can be done manually by technicians. Lastly, it was noted that being a small

company requires just a short period of time for personnel to access the various locations of their physical system. Also, there is also no high or visible dependence from other networks as sometimes happens in companies handling bigger networks.

Finally, another interviewee was quite sceptical about security measures, seeming to think that all that was needed was already in place. Specifically, it was said that they could restrict connections to the enterprise resource planning system (ERP), but this was yet to be done. The reason for not doing it was that there was a need to access the system from anywhere, and that they did not want security measures to get in the way of their access to the ERP, i.e. it was an issue of usability. One of their protection measures was the existence of a 30 days limit for their password, which was required to change by the system after it expired. Passwords were also encrypted. Although the administrator could re-establish a password, he/she was not in any position to know the password. The ERP was said to be very good since it was well-known software and used by several major companies. This was not a product developed by them, and thus, there was a need for many other things to be done in it; hence, security was not their primary priority. Lastly, it was mentioned that the reason why they did not worry about security is because they believed that all the security measures they needed were already in place. In Table 3, we summarize the identified issues, incidents and solutions in the utility provider organization.

Table 3 Resilience: Utility provider

	Utility provider
Issues	Risk seen as low; security is not a priority. Little value or reward to typical hacker. Prioritize usability over protection/security. Not concerned about Internet security risks.
Incidents	Cascade effects and interdependencies.
Solutions	Belief or complacency that all the security measures needed are already in place.

4 Analysis of ethnographic and interview data: the ‘mental models’ used in reasoning about risk

Our first analysis is based on developing an understanding of the ’mental models’ with which organizational members address risks as part of their organizational roles. The elicitation of mental models in risk studies has generally been aimed at uncovering deficiencies in individuals’ understanding of complex risks (for example [2]). But the work on mental models in our project used unstructured interviewing and ethnography to get a more contextualized understanding of exactly how organizational members use particular interpretive schemes, heuristics and other ways of discursive reasoning in order to deal with organizational risks. We have there-

fore developed an analysis that is closer to notions of the social construction of risk and Hilgartner's [9] approach in particular. In this approach, risk objects come into prominence, or recede out of prominence, in a process termed 'emplacement' and 'displacement'. Emplacement occurs typically when the consequences of a risk become magnified in social discourse for some reason, or the causes of risk seem to be less manageable and more likely. Displacement occurs when risk appears to come under greater control. Our primary concern has, therefore, been with how the interpretive themes or models that people exhibit perform this emplacement and displacement. To recap: there were two fieldwork sites: the first, in which an organization operating the utility service was the subject of the work; the second, in which an organization providing an information systems service to a utility was the subject of the work. The two utilities operated in different industries, and were of a very different size and character. The process of analysis was to take the fieldworkers' notes, including interview transcripts, and select fragments that are self-contained and give evidence of some kind of model or schema in a persons explanation of risk in the utility organization they work in. As many of the interviews were not in English, the two fieldworkers translated all notes (including verbatim interview extracts) into English before analysis. The fragments were then coded according to the model or schema, and according to the risk emplacement and displacement process being supported by the model. The codes were then used to gather fragments together, and higher-level codes developed in order to provide a systematic account of the nature of the models and their emplacement and displacement functions.

It is clear that organizational members have a wide variety of models across both technical and social domains. The 'models' are not generally integrated, uniform, self-consistent representations even within individuals. They tend to be, or at least emerge as, fragmentary and partial, and serve as discursive resources to justify a claim as much as resources for reasoning about a claim.

The function in the utility organization was much more often displacement than emplacement, but more emplacement than displacement for the systems organization. The context of the interviews and observations has to be borne in mind, however. Experience of cyber-security risk, in particular, had been much more extensive at one of the sites. Moreover, sometimes emplacement and displacement went together. A risk may be emplaced in order to show how the organization has taken it seriously enough to displace it with strong controls.

One of the fieldworkers argued that one of the fieldwork sites had a clear notion of actual and potential risks. This does not seem coherent logically, as all risks involve some kind of potential for harm, but it clearly mattered to one of the organizations that they could acknowledge that some risk existed, but had reasonable grounds for not devoting resources to managing it. Potential risks were, in some sense, 'theoretical' and 'general' de-contextualized and offering no reason for acting on them in this organization. The fieldworker referred to two 'registers' of risk. At both field sites, cyber-security risks were displaced by other risks being seen as substantially more important.

It is quite hard to categorize the informants' models in terms of whether they produce vulnerability or resilience. Logically, they are inevitably a source of both

enabling people to reach an understanding of a risk but simultaneously constraining the way they do so. The main kinds of model found in the analysis were as follows (see Table 4):

Table 4 Modelling risk

Models
1. Failure path models – sequences of action that lead to some failure state
2. Access and connection models – connectedness of entities in a system and the accessibility of one to another.
3. Functionality and protection models – what a system can do, and its protective function.
4. Technical boundary models – boundaries of responsibility for risk and competence.
5. Experiential narrative models - narratives of incidents, or risks.
6. Ordering models – that puts security risk below other threats and other demands on resources.
7. Frequency models – where frequency becomes a dominant criterion for allocating attention.
8. Cost-benefit models – where risk controls are unnecessary as costs exceed benefits.
9. Responsibility attribution models – where others are responsible for particular risks.
10. Abstract, global attribute models – characterizations of a whole organization or situation.

1. **Failure path models.** These represented sequences of action that led to some failure state. They were generally straightforward, and enabled people to reason about how plausible they were. For example, one informant reasoned that risks were low because of the way an attacker would need certain expertise to gain access to computing devices, and then a different kind of expertise to actuate physical devices.
2. **Access and connection models.** These represented the connectedness of entities in a system and the accessibility of one to another typically the accessibility of some vulnerable entity like data or a physical actuator to some person, some role, some computer or other device. This accessibility was the basis for reasoning about a related risk. Such models were also implicated in statements people made about redundancy in vital links.
3. **Functionality and protection models.** These represented what a system of some kind could do, especially what kinds of protective function it provided. People did not seem to have an explanation, particularly, but simply a representation of a capability or capacity. For example, systems had firewalls, systems blocked certain kinds of access, and systems could produce certain kinds of harm.
4. **Technical boundary models.** These were related to responsibility models (below) but were primarily representations of the technical system as a collection of devices that were strongly partitioned, and typically supplied by different providers. The boundaries represented boundaries of responsibility for risk and boundaries of competence. Sometimes people would say we can only do something about X but not Y to indicate a residual uncertainty about a risk that was partially the responsibility of someone else.

5. **Experiential narrative models.** These were narratives generally of incidents, or materialized risks of some sort. It was often not obvious what these led to: people would offer a narrative without general conclusion, indicating that it was sufficient itself. Narratives are not quite the same as models, not necessarily being representations of something in the world. But they seemed to function as models, providing structured accounts of some issue or problem (in this case security risk) that had come into the discourse. Often the narrative involved emplacing a risk, explaining an event in the recent past, and then displacing it by reasoning about how controls had subsequently been brought in. Logically, the current state of security is described by the current state of the system, but the narrative sequence of some experienced event followed by some remedial action seemed to help people reason about security. In the systems organization there were more failure narratives, with less risk displacement as a conclusion.
6. **Ordering models.** Often the explanation for a lack of interest in certain kinds of risk was based on priority: an ordering that put security risk well below other threats and other demands on resources more generally. In the utility organization, the main risks were seen by some as being commercial, displacing cybersecurity risks; in the systems organization, the main risks were said to be seen as being physical. Ordering models are not of a risk itself, nor of the organization or its resources, but of a problem set that exists in some priority ordering. We tend to think of mental models as representations of the world out there for an individual or group. But, for an action-oriented actor, it may be less important to have a descriptive representation of this kind than to have a list of actions and associated priorities.
7. **Frequency models.** These are closest perhaps to the long-standing concern with the heuristics people use to deal with probabilistic problems. People give evidence in their language of an effort to represent the frequency of different kinds of event, and obviously in the context of risks the frequency becomes a dominant criterion for allocating attention. People often referred to the experience as a way of estimating frequency in a rough way: for example referring to the way in which they had sometimes experienced one kind of problem or failure but never experienced another. An expert, technical observer could easily point to the logical flaws in inferring probability from historical frequency in a non-stationary domain. But people gave no evidence that inferring frequency from experience was somehow problematic.
8. **Cost-benefit models.** People would sometimes reason that risks were low because the costs to an adversary were high and benefits low. This was typically a risk displacement strategy. They also argued that possible risk controls were unnecessary as their cost exceeded their benefit. In this sense, risks could be displaced not by being small but by having solutions that were prohibitively expensive.
9. **Responsibility attribution models.** Patterns of responsibility, often patterns in which others are responsible for particular risks, sometimes appeared to underlie people's responses. Equipment manufacturers, for example, were commonly attributed with responsibility for the security of their products, and from this peo-

ple inferred that risks to those products were therefore low. Responsibility was attributed over time as well as technical and social space. In one case someone displaced security risk by saying relevant decisions were 'made in the past and that we do not worry about this any more'. Occasionally these models incorporated some representation of legal responsibility, but this was not prominent in the data.

10. **Abstract, global attribute models.** These were simple characterizations of a whole organization or situation. Those of the utility organization were more optimistic: for example, some people had a simple model of sufficiency: a general belief that there were enough appropriate controls to nullify risk. In the systems organization these were more pessimistic: characterizing the utility organization it supported as having a culture inappropriate to security in a number of ways. As we suggested, these models could equally be a source of vulnerability or of resilience. It is the specific context and specific manifestation that will be decisive. But it is instructive how wide-ranging the types of model are. They are not just block diagrams in which one semantic element is linked to another. They are qualitatively quite different, and point to the resourcefulness of organizational members coping with a world that is complex not only in having many components but in making many demands on people acting in it. Some of these demands involve having an appropriate representation of a conventional system a network of devices for instance but others involve having an appropriate representation of other peoples expectations and capacities, of norms and conventions, and so on.

This means it will always be insufficient to assess mental models of security in terms of their technical correctness, as it will sometimes be more important to consider how well they represent prevailing social issues and requirements. At one of the field sites, a researcher with ICS cyber-security expertise as a practitioner undertook a penetration test of part of the organization's systems. This produced a technical understanding of some of its vulnerabilities, indicating certain vulnerabilities that the organization had formerly seemed unconcerned about. This, on face value, suggests that the organization members had imperfect mental models or interpretive schemes of the system under their management. But it is important to recognize that such models are adaptations to a wide variety of experiences of which technical experts have no knowledge. They cannot therefore be judged as deficient or otherwise in some general sense. What is more important is that there is an awareness within the system of how those models contribute and detract from its security. As a practical recommendation of this work, we therefore suggest that utility organizations engage in penetration testing and perhaps other forms of vulnerability analysis, not only to discover specific vulnerabilities but also to learn more about the mental models they use, models that are important in shaping these vulnerabilities.

5 Conclusion

What has emerged from our empirical studies of people and organizations, as they struggle with concerns about resilience, is the connection with other issues that have traditionally bothered those interested in the computer-human interface: notably the challenges of dependability, reliability, safety and security. As computer-based systems – embracing humans, computers and engineered systems – become more complex and organizationally embedded, so these challenges involving complex interactions among technologies, organizations and individuals have multiplied. While much of the work on reliability and resilience has naturally focused on major and often catastrophic failures, what has been documented in this research has been some of the more ordinary, everyday instances of failure. Not surprisingly, perhaps, instances of lack of resilience in many settings are not normally catastrophic but are rather mundane events that occasion situated practical inquiry and repair – people work out how to deal with incidents as they occur. Resilience, like ideas about reliability or dependability, can be seen as being the outcome of peoples' everyday, coordinated, practical actions. Workers draw on more or less dependable artefacts and structures as resources for their work of achieving organizational objectives through the interaction between technical systems and human skills. Our empirical studies illustrate that abstract 'rules for resilience – such as procedures, models, proscriptions, prescriptions, etc. – have to be applied within the context of socially organized work settings in which those who have to apply such rules have to deal with whatever contingencies arise. As the International Atomic Energy Authority (IAEA) literature (2006) states 'An important factor in a management system is the recognition of the entire range of interactions of individuals at all levels with technology and with organizations'[11].

This kind of argument and analysis concerning resilience, also links to ideas about reliability, and thereby resolves or modifies, to some extent, the on-going dispute between the idea of the High Reliability Organization (HRO) and the idea of the 'normal accident' [15]. Reliability can be defined as the ability of a system to deliver in the quantity and the quality expected by users. The term High Reliability Organization (HRO) was assigned to a group of organizations that were assumed to operate virtually error-free in risk-laden environments, where failure could lead to disaster [18]. Ethnographic studies conducted on operational nuclear power stations [3, 14], nuclear-powered aircraft carriers [19] and nuclear-armed submarines [1], described the structural mechanisms that were assumed to make HROs dependably safe and reliable. Although characterized by having high degrees of interactive complexity that allowed for system unpredictability and system interdependencies that ensured tight coupling, the HRO structural mechanisms of containment suggested the ability to avoid accidents that might normally be expected – as in Perrow's concept of 'normal-accidents' [15]. As well as macro-analysis of structures at the organizational level, HROs have been assessed in terms of their culture [28]. At the micro-level HROs were assessed in terms of members skills and abilities, and the pattern of heedful interrelations in a social setting that were seen as evidence of a collective mind [29]. From this perspective, people within inherently

risky HROs demonstrated ways of acting and thinking that prevented problems arising, and if things did go awry, were able to contain problems to prevent them from escalating. Resilience, from this perspective, is the ability of organizations to become resourceful in their ability to maintain positive adjustment under challenging conditions [27] and 'bounce back' from untoward, surprising, or disruptive events [8, 30]. Resilience approaches emphasize the idea that disruptive events are complex incidents that occur regularly and that systems should be designed to bounce back quicker and stronger because the impact was less. More resilient systems can withstand disruption, suggesting the idea that there is a flexible continuum between the reliable system and the 'normal accident'. Resilience is: '...the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.' [26].

What emerges from the research and the ethnographic fieldwork is a detailed understanding of the way in which resilience is an essential aspect of the collaborative, social, character of work. Any computer systems that are used, whatever 'technological' characteristics they may have, are thoroughly 'social' (and organizational) in character and thus designing and implementing 'resilience' into distributed and shared systems of work requires that this fundamentally social dimension has to be taken into account. This involves considering the ways in which plans and procedures for resilience, and adjustment to failure, are placed within an appropriate social and organizational context, as elements which enable workers to make sense of their work and come to a decision about future courses of action. Within CSCW research the work of Suchman and others [23, 24, 25] illustrate how important it was to consider the 'fit' of any models of resilience and risk-taking with the ways in which work is actually done. It is people that do the work in organizations, not idealized models or plans. People are 'rule users' rather than merely 'rule followers'. It is the everyday judgment of workers, in interpreting and improvising standard procedures or plans, that gets the work done and prevents or reacts to failure. As our observations suggest, the problem with resilience is that even when presented with instructions that 'anyone' should be able to understand and follow, practical troubles still arise, and users characteristically rush to premature and often mistaken conclusions about what has happened, what is happening, what the machine 'meant', what the machine 'is thinking', and so on. What is also important – as far as resilience is concerned – is some notion of 'awareness' – knowing about, knowing how to use, that information, those artefacts, etc., that are relevant to the accomplishment of work [20, 25]; exercising judgment in light of the various contingencies and uncertainties that arise during the course of work. In this chapter, we have considered the importance of various human and organizational factors in the promotion of resilience. This recognizes the identification of human errors as the greatest threat to cyber-security, and also that humans appear to be highly prone to cyber-attacks, e.g., social engineering and spear phishing attacks. Although a set of guidelines exists in the EU (i.e., EUs cyber incident reporting system), it appears that these are currently not well integrated in all critical infrastructures. Our analysis indicates the need to

put security response teams in place, which eventually will help to improve security awareness as well as resilience in critical infrastructures provisioning.

Acknowledgements This chapter is based on work from COST Action CA15127 ('Resilient communication services protecting end-user applications from disaster-based failures - RECODIS') supported by COST (European Cooperation in Science and Technology), and supported by the European Union Seventh Framework Programme under grant agreement no. 608090: project HyRiM (Hybrid Risk Management for Utility Providers).

References

1. Bierly III, P.E., Spender, J.C.: Culture and high reliability organizations: The case of the nuclear submarine. Journal of management **21**(4), 639–656 (1995)
2. Bostrom, A., Morgan, M.G., Fischhoff, B., Read, D.: What do people know about global climate change? 1. mental models. Risk Analysis **14**(6), 959–970 (1994)
3. Bourrier, M.: Organizing maintenance work at two american nuclear power plants. Journal of contingencies and crisis management **4**(2), 104–112 (1996)
4. Dobson, S., Hutchison, D., Mauthe, A., Schaeffer-Filho, A., Smith, P., Sterbenz, J.P.: Self-organization and resilience for networked systems: Design principles and open research issues. Proceedings of the IEEE **107**(4), 819–834 (2019)
5. Gouglidis, A., Green, B., Busby, J., Rouncefield, M., Hutchison, D., Schauer, S.: Threat awareness for critical infrastructures resilience. In: 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pp. 196–202. IEEE (2016)
6. Gouglidis, A., Green, B., Hutchison, D., Alshawish, A., de Meer, H.: Surveillance and security: protecting electricity utilities and other critical infrastructures. Energy Informatics **1**(1), 15 (2018)
7. Gouglidis, A., König, S., Green, B., Rossegger, K., Hutchison, D.: Protecting water utility networks from advanced persistent threats: A case study. In: Game Theory for Security and Risk Management, pp. 313–333. Springer (2018)
8. Grabowski, M., Roberts, K.H.: Reliability seeking virtual organizations: Challenges for high reliability organizations and resilience engineering. Safety Science (2016)
9. Hilgartner, S.: The social construction of risk objects: Or, how to pry open networks of risk. Organizations, uncertainties, and risk pp. 39–53 (1992)
10. Hutchison, D., Sterbenz, J.P.: Architecture and design for resilient networked systems. Computer Communications **131**, 13–21 (2018)
11. IAEA Euratom, F.I.O.P.U., WHO: Fundamental safety principles: Safety fundamentals (2006)
12. Knowles, W., Such, J.M., Gouglidis, A., Misra, G., Rashid, A.: Assurance techniques for industrial control systems (ics). In: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, pp. 101–112. ACM (2015)
13. König, S., Gouglidis, A., Green, B., Solar, A.: Assessing the impact of malware attacks in utility networks. In: Game Theory for Security and Risk Management, pp. 335–351. Springer (2018)
14. La Porte, T.R., Thomas, C.W.: Regulatory compliance and the ethos of quality enhancement: Surprises in nuclear power plant operations1. Journal of public administration research and theory **5**(1), 109–138 (1995)
15. Perrow, C.: Normal accidents: Living with high risk technologies-Updated edition. Princeton university press (2011)
16. Rass, S.: Decision Making When Consequences Are Random, pp. 21–46. Springer International Publishing, Cham (2018). DOI 10.1007/978-3-319-75268-6_2. URL https://doi.org/10.1007/978-3-319-75268-6_2

17. Rass, S.: Security Strategies and Multi-Criteria Decision Making, pp. 47–74. Springer International Publishing, Cham (2018). DOI 10.1007/978-3-319-75268-6_3. URL https://doi.org/10.1007/978-3-319-75268-6_3
18. Roberts, K.H.: Some characteristics of one type of high reliability organization. Organization Science **1**(2), 160–176 (1990)
19. Rochlin, G.I., La Porte, T.R., Roberts, K.H.: The self-designing high-reliability organization: Aircraft carrier flight operations at sea. Naval War College Review **40**(4), 76–92 (1987)
20. Schmidt, K.: Riding a tiger, or computer supported cooperative work. In: Proceedings of the Second European Conference on Computer-Supported Cooperative Work ECSCW'91, pp. 1–16. Springer (1991)
21. Smith, P., Hutchison, D., Sterbenz, J.P., Schöller, M., Fessi, A., Karaliopoulos, M., Lac, C., Plattner, B.: Network resilience: a systematic approach. IEEE Communications Magazine **49**(7), 88–97 (2011)
22. Sterbenz, J.P., Hutchison, D., Çetinkaya, E.K., Jabbar, A., Rohrer, J.P., Schöller, M., Smith, P.: Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks **54**(8), 1245–1265 (2010)
23. Suchman, L.: Working relations of technology production and use. Computer supported cooperative work **2**(1-2), 21–39 (1993)
24. Suchman, L.: Making work visible. In: The New Production of Users, pp. 143–153. Routledge (2016)
25. Suchman, L.A.: Plans and situated actions: The problem of human-machine communication. Cambridge university press (1987)
26. (US), N.I.A.C.: Critical infrastructure resilience: Final report and recommendations. National Infrastructure Advisory Council (2009)
27. Vogus, T.J., Sutcliffe, K.M.: Organizational resilience: towards a theory and research agenda. In: 2007 IEEE International Conference on Systems, Man and Cybernetics, pp. 3418–3422. IEEE (2007)
28. Weick, K.E.: Organizational culture as a source of high reliability. California management review **29**(2), 112–127 (1987)
29. Weick, K.E., Roberts, K.H.: Collective mind in organizations: Heedful interrelating on flight decks. Administrative science quarterly pp. 357–381 (1993)
30. Wildavsky, A.: But is it true?: a citizen's guide to environmental health and safety issues. Harvard University Press (1997)