Chapter ** (please leave)

Evaluating emergency preparedness: Using responsibility models to identify vulnerabilities

Gordon Baxter and Ian Sommerville

Introduction

Preventing acts of terrorism requires being able to accurately and reliably predict when, where and how the terrorists will strike. When prevention is not possible the aim is to mitigate the severity of the consequences of the terrorist acts. Terrorists normally attempt to cause maximum disruption and achieve significant publicity by attacking systems that they perceive as being of great importance (physically and psychologically). Here we are talking about systems in the most general sense of the term, rather than just technological systems. More particularly, we are talking about socio-technical systems, and encompass both organisations and infrastructure within our broad definition.

The responses to emergency situations, such as terrorist attacks, can be characterised by three common traits (Goughnour and Durbin, 2008):

- The information sources and the people who use them are geographically widely dispersed.
- The information which rapidly changes as the situation develops needs to be made widely distributed as soon as it becomes available (and has been validated).
- The types of information that have to be managed—processed, analysed and reviewed—are quite disparate and may keep changing over time as the situation develops.

We know a lot about the different ways in which terrorists can strike, but often know less about the when and where until it may be too late to prevent at least some damage from occurring. To protect the public effectively against a terrorist attack therefore requires a high degree of emergency preparedness. This is based on co-ordinated functioning, co-operation and communication at global, regional, national and local levels, and multi-agency working (Veness, 2012). The details for how to respond to particular emergency situations are normally laid out in contingency plans. These plans can only be accurate if the relevant people with the appropriate skills work together to develop them. This is because the plans have to cover so many different aspects of the situation, such as how to achieve shared awareness and understanding across the various agencies involved (e.g., Convertino et al., 2011, Wu et al., 2013).

One way of making sure that a system has an appropriate level of emergency preparedness is to learn from other, similar, emergency situations that have happened in the past. The London Resilience Team, for example, developed new plans and established new facilities based on lessons learned in the aftermath of 2005's London bombings (Lewis, 2012). It is also possible to observe and learn from others as they practice emergency management. The Beijing Olympic Games organising committee used this approach. They sent staff to monitor the emergency management operations at the Sydney and Athens summer Olympics, and the Turin winter Olympics so that they could apply what they had learned to the Beijing games (Jiwei et al., 2010).

The notion of responsibility is particularly important when handling emergency situations. When analysing South Carolina's census data on preparedness to deal with terrorism, however, Pelfrey (2007) found that while states were assigned significant responsibilities, most of the relevant federal documents focused instead on goals and objectives. The problem is exacerbated because multiple agencies are normally involved in responding to terrorist attacks so responsibilities are distributed across and within the different agencies.

A better understanding of the way that responsibilities are managed in multi-agency situations is therefore important. There may be some responsibilities that are shared across agencies, for example, and there may be some responsibilities that fit naturally into the remit of more than one agency. Understanding how the different agencies deal with these situations can generate lessons which can be incorporated into contingency plans. This should improve the shared awareness and understanding among the agencies of how responsibilities are managed. In this way it should be easier for agencies to work together in emergency situations, and step in to help each other where appropriate.

In the next section we introduce our conceptualisation of the notion of responsibility. We then go on to describe a graphical technique for modelling

responsibilities that can be used in analysing socio-technical systems. We discuss how it can be used, and illustrate its use with some simple examples. We then identify the classes of vulnerabilities that are associated with responsibilities, as well as those that are associated with the use of resources. We show how responsibility modelling can be used to identify vulnerabilities in contingency plans, before discussing its role in informing the design of table-top exercise scenarios, and shaping the nature of live table-top exercises as they evolve. We conclude by summarising how performing vulnerability analyses (using responsibility modelling) can help improve emergency preparedness.

Responsibility

The tools and techniques available to help analyse failures (e.g., see Leveson, 1995) are often based on concepts such as goals, and describe how these are achieved (or not) using abstractions such as tasks and functions. These tools and techniques are very good at dealing with technical failures, but are less well suited, to dealing with the many failures where the attributed causes lie within the socio-technical system per se. There is some evidence, for example, that the London bombings in 2005 were at least partly attributable to socio-technical failures (Intelligence and Security Committee, 2006). We have therefore been using the notion of responsibilities, which is more abstract than goals and objectives, to express the softer aspects of system performance. It is also a concept that system stakeholders are generally more comfortable with, and find easier to comprehend and discuss.

Our definition of responsibility is a pragmatic one:

> [A responsibility is a] *duty, held by some agent, to achieve, maintain or avoid some given state, subject to conformance with organisational, social and cultural norms. (Sommerville et al., 2009, p.181.)*

In the majority of cases the *agents* that are assigned (or allocated) responsibilities will be people or organizations. The agents could, however, also be a technological device or a software application. If the responsibility is to raise an alarm when smoke is detected, for example, this could be assigned to an automatic smoke detection device.

In order to discharge a responsibility an agent will normally need to utilise some *resources*. These resources can be concrete (such as people or physical objects) or abstract (time, or a piece of information).

Responsibilities are normally discharged in a context in which there are several norms that define and constrain how the agents are supposed to operate. These factors include contingency plans, standard operating procedures, and statutory

regulations, which all affect how responsibilities should normally be discharged.

Responsibility Modelling

We have developed a graphical representation technique called Responsibility Modelling (RM) for analysing systems and organizations. A responsibility model shows how responsibilities are assigned to agents and what resources are needed to discharge responsibilities. The basic concepts are illustrated in Figure 1.

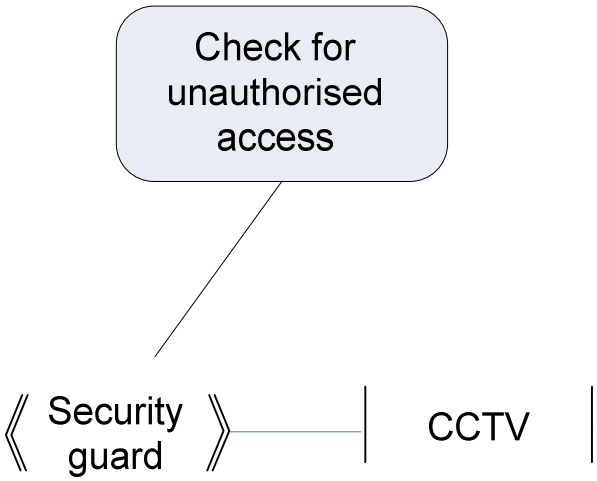

Figure 1. Basic elements of a responsibility model. The agent *Security guard* is assigned the responsibility *Check for unauthorised access* and uses the resource *CCTV* to discharge that responsibility.

Responsibility models can be developed for prospective analysis, as well as retrospective analysis. Depending on the purpose of the analysis, access to resources to create the models in the first place, and the amount of time and effort available to do the analysis, three methods can be used to collect data for the models:

- Stakeholder interviews. Stakeholders are asked about their responsibilities and the resources they use to discharge them.
- Document analysis. Documents such as organizational structure charts, local operating procedures and contingency plans are analysed to identify responsibilities, agents and resources. Some care should be exercised here when interpreting the results: there are usually differences between how the procedures say people are supposed to work, and what people really do in practice (e.g., Dekker, 2006).
- Archive data. Post hoc accident reports and incident debriefings can sometimes be used to identify responsibilities where systems have failed.

To create the model any drawing package can be used, or they can be drawn by hand. The information that has been collected is graphically represented to show how responsibilities are allocated, and how resources are used. For large socio-technical systems, such as those that provide and support Critical National Infrastructure (CNI), it is often easier to present the system as a set of related responsibility models, rather than try to model the whole system in one diagram. Each level of responsibility can be represented by its own responsibility model diagram(s). These models, which reflect the different levels of responsibilities, are usually organised hierarchically. We have found it most useful to focus on particular aspects, rather than try to create a comprehensive model for the whole system. It can be helpful to adopt a risk analysis style of approach here to identify which parts of the system to analyse in detail.

Identifying Vulnerabilities

All systems and organizations contain vulnerabilities. If these vulnerabilities are not identified, they can persist as latent failures in the socio-technical system (Reason, 1990). In other words, they may not be a problem until they are triggered by real events. These latent failures can reduce the resilience of the socio-technical system to events such as a terrorist attack, because when they become active they adversely affect the system's ability to deal with the consequences of that event. One of the benefits of responsibility models is that they can be used to identify potential vulnerabilities in responsibilities, agents and resources.

Responsibility vulnerabilities
There is a set of system vulnerability types associated with responsibilities (and agents), each of which can contribute to system failures. We have extended Sommerville's (2007) original list of six main types of responsibility and agent-related vulnerabilities, based on our subsequent observations.

Unassigned responsibilities
Unassigned responsibilities are probably the easiest type of vulnerability to identify from a responsibility model. An unassigned responsibility is simply one that has not been assigned to any agent. If a responsibility has no links associated with it in the responsibility model, this suggests that there is a vulnerability and that that particular responsibility will not be discharged.

Duplicated responsibilities
Duplicated responsibilities arise when a particular responsibility is assigned to more than one agent. These can arise when systems are decomposed in a way that leads to exactly the same responsibility appearing in separate parts of the system. They can also occur when multiple agencies have to work together, particularly if they are dealing with an acute problem, where the discharging of responsibilities may not always be obvious, leading to one agent attempting to discharge a

responsibility that somebody else is either currently discharging, or has already discharged.

Diffusion of responsibility
The notion of diffusion of responsibility comes from social psychology. Diffusion of responsibility can occur in multi-agency environments when each agency may believe that one of the other agencies has been assigned a particular responsibility. The net result is that nobody discharges the responsibility because they expect another agency to do it. This vulnerability includes elements of unassigned responsibilities and duplicated responsibilities and is specific to multi-agency requirements.

Uncommunicated responsibilities
Often responsibilities are associated with roles, and an agent may have several roles. Uncommunicated responsibilities arise when an agent that who has been assigned a particular role is not told about the responsibilities that are associated with that role.

Misassigned responsibilities
Sometimes an agent may not have the capabilities (knowledge, skills and attributes) or resources to discharge the assigned responsibility. In this case, it is described as a misassigned responsibility. These can occur when a situation evolves in such a way that responsibilities are (re-)allocated to those agents that are available at that point in time so that they can be discharged, rather than waiting for the originally allocated agent to become available.

Responsibility overload
When an agent is assigned several responsibilities they may not have the physical or mental capacity to be able to discharge all of those responsibilities within the required time frame. This situation is described as responsibility overload.

Responsibility fragility
Also described as responsibility brittleness, responsibility fragility occurs when a particular responsibility is assigned to an agent, but if that agent is not available, there is no back-up agent who can discharge that responsibility. This sort of situation arises when a responsibility is assigned to a named individual (e.g., Bob, or the Health and Safety Officer) because they have the particular capabilities to discharge it, and that individual happens to be absent or unavailable for some reason.

Responsibility conflict
Sometimes agents have to fulfil multiple roles within an organization and the responsibilities associated with those roles may conflict. If, for example, a person has the responsibility for managing a project (making sure it is delivered on time and within budget), but also has the responsibility for technical assurance of that

project (making sure that the application or system has been rigorously developed, tested and so on), these two responsibilities are likely to come into conflict.

Resource Vulnerabilities

The vulnerabilities associated with resources relate to their production and consumption, and their availability and accessibility. If an agent consumes a particular resource to discharge some responsibility, for example, then this resource has to be provided somehow. If the resource is produced by another agent, this indicates that that agent should be assigned the responsibility to produce that resource.

If an agent needs to use information resources to help them discharge their responsibility as part of the response to an event such as a terrorist attack, consideration must be given to how that agent accesses these resources. If the information resource is only available online, for example, and the network connection to that resource has been wiped out, the agent will be unable to discharge that particular responsibility unless they can access the required information by other means.

If an agent has to use physical resources, such as transport for relocating or evacuating people after a terrorist attack, consideration has to be given to how to access that transport. If the road network becomes blocked or even destroyed, for example, this may make it impossible to get access to the transport vehicles.

Managing Vulnerabilities

In an ideal world, there would be a perfect match between responsibilities, agents and resources. Responsibilities would always be discharged in a timely manner by agents with the appropriate combination of knowledge, skills and attributes. The way that responsibilities get discharged on the ground, however, will often diverge from written procedures and plans. Part of the reason for this is that procedures and plans cannot cover the contingencies of all possible situations. What usually happens is that people will adapt the plans and procedures to deal with the particular situations at hand.

Managing the different types of responsibility vulnerabilities may not always be straightforward. Duplicated responsibilities, for example, are a vulnerability, but a system can be made more resilient if back-up agents are assigned to critical responsibilities. The secondary agents must understand, however, when and how they should step in to discharge those responsibilities.

Similarly, a misassigned responsibility will not necessarily be discharged ineffectively (if at all). As an event unfolds, some agents may become unavailable for various reasons. This may mean that their assigned responsibilities get dynamically re-assigned to one of the available agents (rather than waiting for the original agent). In these situations the inherent flexibility and adaptability of people

often means that some way will be found to discharge that responsibility, at least partially, using workarounds as appropriate.

Agents will usually be assigned several responsibilities. The way they often deal with this is to assign a priority to each of their responsibilities and focus on those with the highest responsibility first. These priorities may be changed dynamically as events unfold, however. In the aftermath of an event such as a terrorist attack, the system has to operate using the available means. Some agents may therefore end up being assigned responsibilities that they do not have the required competence to be able to fully discharge. The decision about prioritising and possibly postponing (or abandoning) a particular responsibility has to therefore consider whether the available (scarce) agents and resources might be better deployed elsewhere to discharge other, possibly more important responsibilities.

Some responsibilities have deadlines. It is therefore important to consider how agents should deal with these. If a responsibility is discharged too early, for example, there may not be any adverse consequences. If that responsibility is not discharged before its deadline, however, consideration should be given to whether that responsibility should be abandoned. If abandoning it would bring the system to a halt, there may be some merit in carrying on after the deadline, even if this means that the system provides a degraded level of service.

Problems can also arise when synchronisation of the discharging of responsibilities is necessary. An agent may have the responsibility for keeping up to date an information resource used by a second agent. The second agent may therefore need to be kept informed of any changes to the information resource, so that they do not end up using old information to make responsibility related decisions that are sub-optimal. This could mean that that responsibility is discharged ineffectively, because any actions based on those decisions may turn out to be incorrect and have to be undone at some later stage.

Identifying vulnerabilities in contingency plans

Contingency plans are normally designed with a view to ensuring the resilience of a system. In other words, they are designed to help ensure that the system keeps running (possibly at a reduced level of service) when a major event (accident, incident, failure, attack etc.) occurs. It is now widely accepted at national levels that CNI, for example, needs to be resilient, and quickly restorable to normal use in the event of failures (e.g., The Scottish Government, 2011, The UK Government Cabinet Office, 2011).

The way to achieve resilience involves making sure that responsibilities in contingency plans are allocated and discharged appropriately and in a timely manner. Unfortunately, however, contingency plans are often inconsistent and incomplete and contain vulnerabilities. These vulnerabilities can be identified using responsibility modelling (e.g., Lock et al., 2009a).

Figure 2, for example, shows part of the model that was created by analysing the flood contingency plan for Carlisle in the UK. The model focuses on the responsibilities associated with the evacuation of people from properties.

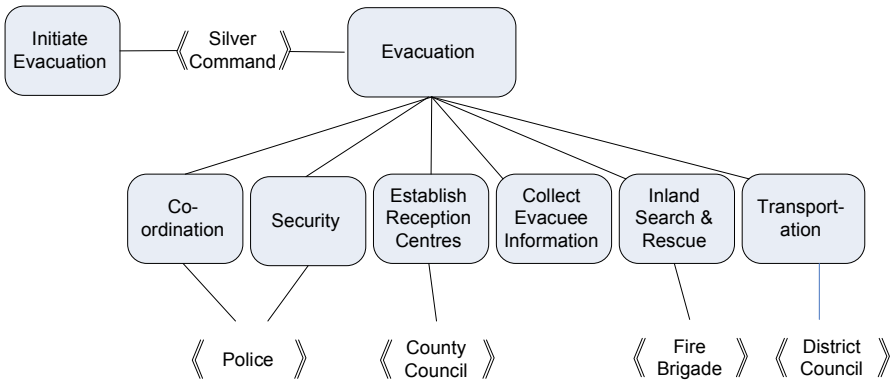

Figure 2. High level responsibility model for flood evacuation plans in Carlisle, England. Responsibilities are shown as shaded rounded rectangles (e.g., *Co-ordination*), and the agents are shown in angle brackets (e.g., *Police*)

If we examine Figure 2 more closely, we can see that all the lower level responsibilities have been allocated to an agent, except for the responsibility *Collect Evacuee Information*. This unallocated responsibility was not obvious in the textual contingency plan, but drawing the responsibility model highlighted this potential problem. In this case, we might expect that one of the agencies (*Police*, *District Council*, etc.) would have been assigned the responsibility to collect the evacuee information. A failure to collect this information could have led to a situation in which the emergency services kept revisiting high risk properties (schools, nursing homes and so on) that had already been evacuated.

Figure 2 shows high level responsibilities, which is why resources are omitted. In Figure 3, the responsibility *Initiate Evacuation* (from Figure 2) has been elaborated to show the resources that *Silver Command* needs to discharge it. The decision to initiate an evacuation is made using information that comes from a risk assessment and flood warnings that are both issued by the *Environment Agency*.

The directional arrows between agents and resources indicate how those resources are used. In Figure 3, the arrows point into the resources *Risk Assessment* and *Flood Warning* from the *Environment Agency*. This shows that the Environment Agency produces those resources. The fact that the arrows from these resources point into *Silver Command* shows that *Silver Command* reads these resources (and subsequently uses the information in them to initiate an evacuation).

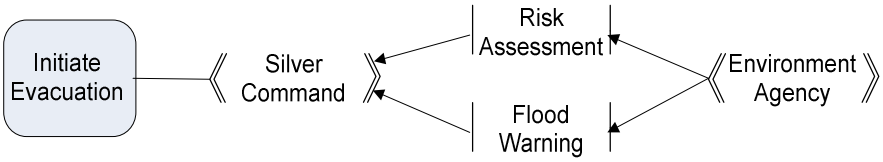

Figure 3. Responsibility model showing resource associations. (Note that the responsibility for the *Environment Agency* to produce the *Risk Assessment* and *Flood Warning* information resources has been omitted for simplicity)

Even though the example in Figure 3 has been somewhat simplified, it illustrates how responsibility modelling can be used to identify vulnerabilities, such as unassigned responsibilities. The models provide a common representation that can be used by stakeholders as a basis for discussing various aspects of how the system works.

Testing contingency plans with table-top exercises

We have already noted that contingency plans contain vulnerabilities. Once contingency plans are written they therefore need to be exercised, tested and re-tested to make sure they are effective in maintaining business continuity (Duncan et al., 2011). In practice, the level of testing of these plans varies somewhat. The CPM and Strohl 2002 survey (cited in Cerullo and Cerullo, 2004), for example, showed that, of the organisations surveyed:

- 15% performed only IT specific tests on their business continuity plans
- 8% performed table-top walkthroughs
- 8% performed call list tests, business unit tests or enterprise, full-scale tests
- 58% used a combination of these three methods
- 10% did not test their plans at all

Exercises such as table-top simulations, and tactical decision games (Crichton and Flin, 2001) normally involve evaluating the use of contingency plans in a simulated emergency. The exercises are used to develop and refresh the knowledge and skills needed to deal with emergency situations: judgement and decision making; developing shared understanding of problems; and building up patterns of known problems (so they can be both identified and responded to more quickly in the future).

The utility of table-top exercises has been illustrated by Jarrett's (2003) assessment of the "Pale Horse" bioterrorism response exercise and Hallett's (2010) discussion of managing waterfront security in Australia. Although Jarrett focused mostly on issues related to dealing with casualties, both he and Hallett noted several general

lessons about the problems that arise when people with different backgrounds and objectives have to co-operate and collaborate in a high pressure environment. In particular they highlighted problems of multidisciplinary communication; who has authority over what; and the control and dissemination of information. Hallett also noted that the exercises have helped to establish working optimal communication channels between participants and increased the understanding of how other organisations are likely to respond to a particular situation.

Table-top exercises are often conducted manually, but can be supported or even completely implemented using technology. Mooney et al., (2012), for example, describe a relatively lightweight, low cost table-top exercise software application, eTableTop, that was developed to help train UK police how to handle major incidents. At the other end of the scale, virtual world simulation technologies are being used to train security staff and emergency responders to deal with terrorist activity (e.g., see Stedmon et al., 2012 for a brief review)

Designing and planning scenarios for table-top exercises is a major undertaking. The scenarios need to be credible and sufficiently simple that they can be handled using the available resources, whilst being difficult enough to present a challenge to the participants (Lacoursiere, 2006). There have been some efforts to support the automatic development of table-top exercise scenarios. The CyberSMART tool (Marshall, 2009), for example, is used to collate data from multiple sources, and then supports the use of that data in developing exercises. Similarly, Payne and Koch (2011) focus on the collection and analysis of data in an organisation's security plan. The organised data is then used to inform a table-top exercise.

We believe there is a role for responsibility modelling here. The responsibility vulnerabilities and risks of a particular system configuration can be analysed by combining responsibility modelling with keyword-based approaches, such as Hazard and Operability Studies (HAZOPS; Kletz, 1999). A systematic approach is used, adapting standard HAZOPS keyword phrases such as "Too early", and "Too late". The analyst takes a checklist of the keyword phrases and applies them to each of the different elements of the responsibility model in turn (Lock et al., 2009b) to examine the possible consequences (and the probability of those consequences occurring). Table 1 illustrates how the keywords are interpreted for responsibilities. This approach allows the analyst to ask "what-if?" questions, such as "What if this responsibility is discharged too early?" and "What if this resource is not available?" The answers to these questions can then be used to help define the scenarios for table-top exercises.

Table 1. Keyword interpretations for categories of hazards associated with responsibilities that should be considered during vulnerability analysis (adapted from Lock et al., 2009b)

Keyword	Interpretation
Early	What would happen if the responsibility was discharged before the required time?
Late	What would happen if the responsibility was discharged after the required time?
Never	What would happen if the responsibility was never discharged?
Incapable	What would happen if the agent did not have the capability to discharge the responsibility?
Insufficient	What would happen if the responsibility was not fully discharged?
Impaired	What would happen if the responsibility was discharged incorrectly?

The vulnerability analysis can be performed on the contingency plan for a terrorist attack. This will help to highlight those parts of the plan that need to be tested, and how they should be tested. If there is an unassigned responsibility identified, for example, then a scenario should be designed to create the situation where that responsibility has to be discharged to see how the system copes.

The responsibility models can also be used to influence how the scenario evolves during the table-top exercise. The models show how agents use particular resources to discharge their responsibilities. One way this could be used is to look at the models, and identify a responsibility that is deemed to be critical to a successful response to a terrorist attack. Then, during the table-top exercise, access to the resources used to discharge that responsibility could be removed or limited in some way (to simulate a network communication failure, for example).

Summary

Emergency preparedness is recognised as the best defence to deal with the threat of terrorist attacks. Emergency situations are characterised by disparate types of dynamically changing information that has to be managed and distributed to widely dispersed users. The way that emergency situations should be handled is normally documented in contingency plans. These plans invariably contain several vulnerabilities. Identifying these vulnerabilities through responsibility modelling is just one way of improving emergency preparedness.

We consider the creation of responsibility models to be the start of the process, rather than the end. The models provide a common representation that can be used as a basis for discussions between stakeholders. This has the potential benefit of bringing together multiple agencies without the pressures that are intrinsic to any

emergency situation. This should help to develop and facilitate communication and shared understanding of problems and responsibilities between agencies.

The process of creating responsibility models is relatively straightforward, and does not require highly specialised skills. Anyone who has a basic understanding of risk management, and can use a drawing package (or even draw freehand) should be able to create a responsibility model. We believe that appropriate tools are needed, however, and have developed a standalone web based tool that can be used to create responsibility models.

Understanding the vulnerabilities associated with responsibilities, and being able to identify them is useful in three ways. First it makes it easier to identify problems within contingency plans so that they can be appropriately managed. Second it provides a basis for creating scenarios for exercising the contingency plan (in a table-top exercise, for example) to examine how responders manage in the face of the identified vulnerabilities. Third it provides suggestions about how particular vulnerabilities can be introduced during live table-top exercises (e.g., by removing an agent, or removing access to an information resource).

Systems and organisations evolve over time. As they adapt to counter changes in the threat posed by terrorists, contingency plans will be changed accordingly. This means that responsibilities will evolve, and responsibility models (and vulnerability analyses) will therefore need to be updated. We believe this is a small price to pay, however, for helping maintain the maximum level of emergency preparedness to deal with terrorist threats.

References

CERULLO, V. & CERULLO, M. J. (2004) Business continuity planning: A comprehensive approach. *Information Systems Management,* 21**,** 70-78.

CONVERTINO, G., MENTIS, H. M., SLAVKOVIC, A., ROSSON, M. B. & CARROLL, J. (2011) Supporting common ground and awareness in emergency planning management: A design research project. *Transactions on Computer-Human Interaction,* 18**,** 1-34.

CRICHTON, M. & FLIN, R. (2001) Training for emergency management: tactical decision games. *Journal of hazardous materials,* 88**,** 255-266.

DEKKER, S. (2006) Resilience engineering: Chronicling the emergence of confused consensus. IN HOLLNAGEL, E., WOODS, D. & LEVESON, N. (Eds.) *Resilience engineering: Concept and Precepts*. Aldershot, UK, Ashgate.

DUNCAN, W. D., YEAGER, V. A., RUCKS, A. C. & GINTER, P. M. (2011) Surviving organizational disasters. *Business Horizons,* 54**,** 135-142.

GOUGHNOUR, D. A. & DURBIN, R. T. (2008) Device independent information sharing during incident response. *Proceedings of IEEE Conference on Technologies for Homeland Security*. Waltham, MA, IEEE.

HALLETT (2010) Australian perspectives on waterside security. *Proceedings of the international waterside security conference (WSS)*. IEEE.
INTELLIGENCE AND SECURITY COMMITTEE (2006) Report into the London Terrorist Attacks on 7 July 2005. Norwich, UK (c) Crown Copyright.
JARRETT, D. (2003) Lessons learned: The "Pale Horse" bioterrorism response exercise. *Disaster Management & Response,* 1**,** 114-118.
JIWEI, Z., LIGONG, T., XUQING, X., HONG, Z. & ZHIGUO, Z. (2010) The emergency management experience of Beijing 2008 Olympic games. *Proceedings of 2010 IEEE international conference on emergency management and management sciences (ICEMMS)*. Beijing, China, IEEE Press.
KLETZ, T. (1999) *HAZOP and HAZAN: Identifying and assessing process industry standards* Rugby, UK, Institution of Chemical Engineers.
LACOURSIERE, J. P. (2006) A risk management initiative implemented in Canada. *Journal of hazardous materials,* 130**,** 311-320.
LEVESON, N. (1995) *Safeware: System safety and computers,* Wokingham, UK, Addison-Wesley.
LEWIS, S. (2012) Emergency preparedness - working in partnership. *Journal of Terrorism Research,* 3**,** 13-16.
LOCK, R., SOMMERVILLE, I. & STORER, T. (2009a) Responsibility modelling for civil emergency planning. *Risk Management,* 11**,** 179-207.
LOCK, R., STORER, T., SOMMERVILLE, I. & BAXTER, G. (2009b) Responsibility modelling for risk analysis. *Proceedings of ESREL 2009*.
MARSHALL, J. (2009) The cyber scenario modelling and reporting tool (CyberSMART). *CATCH '09 Proceedings of the 2009 Cybersecurity Applications & Technology Conference for Homeland Security* Washington DC, IEEE Computer Society.
MOONEY, J. S., GRIFFITHS, L., PATERA, M., ROBY, J., OGDEN, P. & DRISCOLL, P. (2012) An electronic tabletop 'eTableTop' exercise for UK police major incident education. *Proceedings of the 12th IEEE international conference on advanced learning technologies*. Washington, DC, IEEE Computer Society.
PAYNE, P. W. & KOCH, D. B. (2011) A Counter-IED Preparedness Methodology for Large Event Planning. *Proceedings of the IEEE International Conference on Technologies for Homeland Security*. Washington, DC, IEEE.
PELFREY, W. V. (2007) Local law enforcement terrorism prevention efforts: A state level case study. *Journal of Criminal Justice,* 35**,** 313-321.
REASON, J. (1990) *Human Error,* Cambridge, UK, Cambridge University Press.
SOMMERVILLE, I. (2007) Models for responsibility assignment. IN DEWSBURY, G. & DOBSON, J. (Eds.) *Responsibility and dependable systems*. London, UK, Springer.
SOMMERVILLE, I., STORER, T. & LOCK, R. (2009) Responsibility modelling for civil emergency planning. *Risk Management,* 11**,** 179-209.
STEDMON, A., LAWSON, G., SAIKAYYASIT, R., WHITE, C. & HOWARD, C. (2012) Human factors in counter-terrorism. *Proceedings of 4th International Conference on Applied Human Factors and Ergonomics*. USA Publishing.

THE SCOTTISH GOVERNMENT (2011) *Secure and Resilient: A Strategic Framework for Critical National Infrastructure in Scotland,* Edinburgh, UK, The Scottish Government.
THE UK GOVERNMENT CABINET OFFICE (2011) *Keeping the Country Running: Natural Hazards and Infrastructure,* London, UK, The UK Government Cabinet Office: © Crown copyright, 2011.
VENESS, D. (2012) Introduction: emergency preparedness. *Journal of Terrorism Research,* 3**,** 3-5.
WU, A., CONVERTINO, G., GANOE, C., CARROLL, J. M. & ZHANG, X. (2013) Supporting collaborative sense-making in emergency management through geo-visualization. *International Journal of Human-Computer Studies,* 71**,** 4-23.