Original Article

The threat management assessment and response model: A conceptual plan for threat management and training

Corinne Peek-Asa[a,*], Carri Casteel[a], Eugene Rugala[b], Christina Holbrook[c], David Bixler[d] and Marizen Ramirez[a]

[a]College of Public Health, Injury Prevention Research Center, University of Iowa, 145 N. Riverside Dr, S143 CPHB, Iowa City, IA 52242, USA.
[b]Eugene A. Rugala & Associates, LLC, Beaufort, SC 29902, USA.
[c]The Boeing Company, Seattle, WA 98124, USA.
[d]The Boeing Company, Huntington Beach, CA 92647, USA.

*Corresponding author.

Abstract Many organizations are implementing threat management approaches to identify and respond to potentially threatening behaviors, threats and acts of violence. Threat management teams bring together different types of expertise throughout a company to assess, investigate, respond to, monitor and mitigate situations. This article presents a conceptual model for threat management and tests the model using tabletop scenarios with a large multinational company's threat management team training program. The tabletop training using the model assisted teams in assessing the incident to determine the risk level, identifying investigative steps, and using expertise and resources of the different team members. Pre-post tests indicated that the training significantly increased team member's confidence in the threat management process.

Security Journal (2017) **30,** 940–950. doi:10.1057/sj.2015.14; published online 6 July 2015

Keywords: workplace violence; prevention; conceptual approach

Introduction

Workplace violence is one of the leading causes of workplace death and traumatic injury in the United States. Violent events cost businesses nearly US$40 million annually, and the personal losses are unmeasurable (Lyncheski and Hardy, 2001; Harrell, 2011; BLS, 2013). For small or medium-sized businesses, a fatal violent event can ultimately cause the business to close permanently. It is thus not surprising that employers in the United States have identified security and workplace violence prevention as one of their top three business priorities (Pinkerton, 2002; BLS, 2006; Securitas, 2014).

Workplace violence can take many forms: violence between employees, violence from customers or clients, violence because of personal relationships such as intimate partner violence (domestic violence)/stalking and violence from crimes such as robberies

(University of Iowa, 2001). How can a company prepare for so many different types of threats; and what can a company do when a potentially violent situation is identified?

The foundation for mitigating these threats is to identify problems early in the process and to have a system in place to respond. The risk for imminent violent situations is fairly small for most businesses, but the potential for threats from internal or external sources exists for all businesses, and thus businesses are challenged to have the right expertise without over-committing resources and personnel (BLS, 2013). For example, surveys have reported that anywhere from 7.8 to 34.5 per cent of workers reported being bullied or harassed in the last year (Zapf *et al*, 2011; Alterman *et al*, 2013). Many companies have implemented Threat Management Teams (TMTs) to bring together the right personnel who can respond to and mitigate threatening behavior, threats and acts of violence, and some research has examined threat management approaches (for example, Meloy and Hoffmann, 2013).

TMTs include members from multiple disciplines (for example, security, human resources, health services, employee assistance program and the law department) within an organization who work together to reduce threatening behaviors, threats and acts of violence and its consequences. One of their primary roles is to identify, investigate and respond to potential threats (Rugala and Isaacs, 2004; Drew, 2005; ASIS SHRM, 2011). TMTs can also play an important role in primary prevention, such as providing training to managers and employees, through establishing outreach programs with local law enforcement and other agencies, helping to establish a workplace culture that is respectful and encourages open communication. The focus of this article, however, is on the TMT role in early identification and response to situations that could lead to potential acts of violence. One key to a successful response is having a team that works well together. For example, the members need to be familiar with each other's expertise and respect each other's contribution, and they all need to know how the company's policies and procedures define how the process should be administered.

Once a company has identified the individuals who have responsibility for responding to a threatening behavior, threats and acts of violence, the team needs to be trained in carrying out an organized and cohesive response. This article presents the Threat Management Assessment and Response Model, developed by the team of authors, which helps guide decisions when a situation of concern arises (it was not developed for acute crises, such as an active shooter). We provide an example of how companies can use this model for training and preparedness. This model identifies the phases and activities that will lead to a coordinated response when an incident and/or concern is identified.

The threat management assessment and response model: A conceptual model for responding to potentially threatening behaviors, threats and acts of violence

Threatening behaviors, threats and acts of violence can be very stressful because they often require quick action, but the action must be appropriate to the situation and the level of threat. These incidents often involve multiple parties and work units. When a threat management incident is reported, key individuals within the business need to be informed of the incident and what actions are being taken. For example, managers and supervisors of the involved employees; organizations that could be involved in the response, are security, human resources, legal and the employee assistance program (EAP), also need to be kept apprised of the incident as it unfolds. The process can feel very chaotic if there is not an underlying plan.

The Threat Management Assessment and Response Model defines elements of a comprehensive response (Figure 1). The model divides a comprehensive response into four major phases and four ongoing actions. The actions in our model have been discussed previously in the literature, and our model provides a conceptual approach to integrate these steps based on experiential research within a multinational company (Borum *et al*, 1999; White, 2013). The four phases identify the progression of a response and include the initial assessment, investigation, intervention/referral and debrief/follow-up/monitor. Actions describe different activities that should be done repeatedly throughout each phase. These actions include assessment of the level of threat, notification, consultation and documentation:

- *Assessment of the level of Threat* involves the identification of the level of threat as low, medium, high or imminent, which often defined specifically in company policy. The threat level can change, sometimes quickly, as the case progresses (as new information is gathered, confirmed and/or developed); therefore, the assessment of the level of threat should be repeated often.
- *Notification* involves informing relevant company units of the current status and activities. Company policy should guide teams on who should be notified with information as the case progresses through the different phases. Notifications can vary based on the specific incident, but can include managers, supervisors, human resources, security, health services, legal and EAP.
- *Consultation* involves providing expertise and guidance to key individuals involved in the case. For example, the TMT can provide consultation to managers or to the work unit on resources available. Consultation also involves bringing in external expertise to the team as it is needed. For example, the team may need to consult with local law enforcement or threat assessment professionals (Peek-Asa *et al*, 2013).

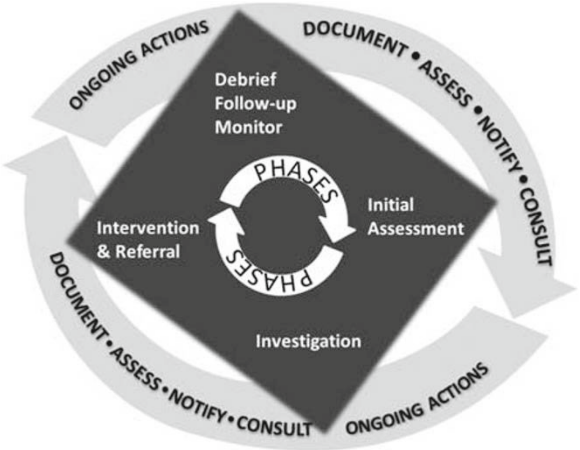

Figure 1: Threat management assessment and response model.

- *Documentation* involves preserving, in writing, information that is collected, from intake, to investigation, to case management using appropriate company databases and other resources. Documentation should also include the decisions that are made and why; who is notified and when; and, what types of actions are taken and who is responsible for them (White, 2013).

The four phases in a case begin with an initial assessment, which occurs when the case is brought to the attention of the TMT Leader and/or a TMT member. An initial assessment can be done by the TMT Leader based upon the facts and circumstances known at that time. If after assessing the case, the TMT Leader determines that the incident is a low risk, the case would be referred back to a single unit such as human resources and management within the business to handle, and the TMT would still be available to provide consultation to the unit in how to deal with the case. If the case warrants further investigation, based on a medium or higher threat level, the next phase is to begin the process of investigation.

The investigation phase of the case involves collecting information about the facts and circumstances of the case in order to understand multiple perspectives and provide a summary of the investigation and possible expected conduct/rule violations to the TMT. The investigation will bring together information sources such as past records (work history, prior corrective action and other information that would assist in assessing the case) from human resources, management or security; interviews with the victim, subject, management and witnesses; applicable company policies and procedures; and relevant information from external agencies (such as local law enforcement). This step by nature will involve many units within the company, and is important to conduct the ongoing actions that include documentation of the information collected, notification and consultation to specific parties that need to be aware of the case (for example, managers and supervisors, or TMT members), and ongoing assessment of the threat level based on the accumulating information. Consultation may include internal or external resources, such as local law enforcement or threat assessment professionals.

Once a sufficient investigation has been conducted, the TMT would then be able to discuss and identify what recommended actions need to be taken to mitigate the threat by putting interventions or referrals in place. These can include referrals to the EAP and/or an external resource, corrective action, or termination of employment. Interventions are often conducted by company units or external agencies that are not part of the TMT, such as law enforcement or victims' assistance programs, and the TMT must have plans to follow-up with interventions put in place with the units that implement them. For example, if an employee has a mandatory referral to EAP, the TMT must have a process for following up to collect appropriate and relevant information about the intervention and its outcome. Often, interventions need to be put in place before the investigative steps are complete. For example, an employee who is being stalked should have a personal safety plan put in place even if the identity of the stalker is not yet confirmed. The interplay between investigation and intervention is coordinated by the TMT through the activities of threat assessment, notification and documentation. During the process, attention to issues of confidentiality and management of information should be guided by company policies, many of which may be driven by local, state or federal laws. If such policies are not in place, teams need to discuss how they will manage information and protect confidentiality of involved parties.

The final step in a case is to debrief, follow-up and monitor. This phase begins when active investigation is completed and interventions are put in place. While the active portion of the investigation is complete, cases are not completely closed; rather they are monitored on a regular basis for any new developments or concerns. At this point, documentation, notification and consultation need to be conducted to ensure that all units are aware of the actions taken and the outcomes, and any responsibilities to follow-up or monitor the case are clearly communicated. For example, if an employee has had their employment terminated because of the threatening behavior or an act of violence against the company or company employees, the appropriate units within the company should be informed of the situation and instructed to report to security immediately if the individual communicates with others at the company or is on company property. Even if the current threat level is low, the TMT should periodically assess the current status to be sure that the threat level has not changed.

How can a business use the threat management assessment and response model?

In order for this model to work most efficiently, a company must first identify individuals who have responsibility for taking action when an incident arises, such as a multi-disciplinary 'Threat Management Team' (TMT). TMTs may include members from various disciplines such as human resources, the law department, health services, the employee assistance program (EAP) and security. TMT may include *ad hoc* members such as labor relations, communications and management, as needed to support a case. Team members may have no prior expertise in workplace violence prevention or response, but their job role is one that makes them an essential partner. For example, human resource professionals have insight and access to information about employee's histories, and they are familiar with company policies that govern employee behavior. They also have expertise in handling confidential employee information. Team membership may vary based on the organization of a company, but the strongest teams will bring in multiple perspectives. A multi-disciplinary approach offers the most comprehensive response. Even if the company does not have a team, it is still important to know who is responsible for mitigating threatening behaviors, threats and acts of violence. Once these individuals are identified, it is important that they are trained together so that they have a mutual understanding of their responsibilities as outlined in the company's policy, each other's role and how to respond. This will ensure a timely and coordinated response.

One effective method for training TMTs is the use of tabletop scenario exercises. Tabletop exercises have been used extensively in disaster preparedness to train responders to effectively carry out their duties and to develop an organized and coordinated response (Chi *et al*, 2001; DHS, 2003; FEMA, 2003). Tabletop exercises have been successful for disaster preparedness because disaster events are rather unpredictable, offer few opportunities to practice responses and require many individuals to work in coordination. Although usually smaller in scale, workplace violence threats share many of these same characteristics, and thus simulated practice in responding to potential threatening behavior, threats and acts of violence is easily adaptable from models in the disaster preparedness community. Tabletop training has been used in workplace violence training, but few evaluations are available (Atack *et al*, 2012; Gillespie *et al*, 2012).

Case study: A tabletop scenario training using the threat management assessment and response model

In a tabletop exercise, a scenario is presented to the TMT, and the team discusses the priority actions and who will carry them out. This example is adapted from training sessions conducted with the TMTs of a large multinational company (the company included 28 of their TMTs in the training; TMTs located throughout the company). The exercise was developed by the authors and pilot tested with the company's TMTs in 2009.

The tabletop scenario exercise was included as part of the company's TMT annual regional training in 2010. Five training sessions were conducted throughout the United States, and the tabletop exercise comprised one half day of the two-day training. The training included 28 multi-disciplinary TMTs that included a combination of security, human resources and other occupations such as health services, the law department, EAP and external partners. Each team had at least one representative from security, human resources, EAP and at least one other unit. In three instances, teams that did not have complete attendance were combined to ensure full representation, but otherwise participants were working with their own TMTs. A total of 251 TMT members participated, with an average of nine members per team. Although the company has conducted TMT training for many years, the training had not used tabletop exercises before the 2009 pilot study.

Teams were provided with complete instructions and were guided through the exercise by facilitators (E. Rugala, C. Peek-Asa, C. Casteel and M. Ramirez). These facilitators are not company employees and were present for the purposes of training only. One facilitator (E. Rugala) is a paid workplace violence expert consultant of the company; the three other facilitators are not paid by the company. At different points as the scenario unfolded, individuals and/or teams were provided worksheets to systematically record plans for next steps, provide a rationale for next actions and to identify different company policies and procedures that helped guide them. Worksheets collected information from both individuals and teams. For information collected at the individual level, individuals filled out their own worksheets that were collected by facilitators and teams were then asked to fill out the worksheet together. Following each step, a discussion was led by the facilitators to identify approaches and to bring the teams together. Each team identified a recorder to collect information, and worksheets were collected before the facilitated discussion. At some junctures, the team's responses dictated what information was provided next. The information for this example focuses on the early phases of the tabletop scenario.

The tabletop scenario initially presented the following situation:

> An employee walked into the break room and saw that a threat against another worker had been spray painted on the wall. The threat said: "*Tom Cavanaugh* [an employee of

> the company] *is a lying sack of #$*%. You* ***will*** *be sorry!*" The employee brought the vandalism to the attention of his manager.

According to the Threat Management Assessment and Response Model, the first phase requires an initial assessment in which the TMT identifies the level of threat. If the TMT does not have at least a general agreement about the level of the threat, the team members of different teams might respond with different degrees of priority and urgency, which can create confusion. Generally, a consistent response is one in which teams follow company guidelines to take comprehensive and appropriate steps in response. Consistency does not mean that the exact same steps are taken in every situation – a well-trained team will react efficiently to the many different types of situations that can arise.

The 28 teams assessed the level of threat differently, and approximately one-third of the teams could not come to an agreement (Figure 2). Company policies can be very helpful in guiding TMTs on assessing risk, and tabletop exercises can be helpful in giving the team practice in coming to consensus. Once the TMTs assessed the level of threat, the facilitator of the scenario discussed the different issues considered by various TMTs when ascertaining the level of the threat. These include identification of a specific person of interest, language that did not express a direct threat but that was clearly threatening in nature and the threat coming from an unknown source. This company's policies would indicate that the level of threat was medium on a range from low to imminent and that an investigation should be conducted.

Once the initial assessment is conducted, a plan of action can begin. Although there is often a rush to begin investigating the situation, it is important to first complete all of the actions: *document* what has happened, for example, by taking photos of the wall; *notify* the head of Security and other key company leaders, as appropriate, by informing them of the allegations and on-going investigation; and *consulting* with involved parties, such as by helping the manager communicate with the workers of the unit.

The investigation phase for any case will likely involve many steps. Some of the steps identified by the 28 TMTs in the training included interviewing workers in the unit to find out if anyone knows who spray-painted the wall, reviewing human resources, management and security records to see if there was any documented history in the unit (for example, employees with security or HR records indicating a history of behavior issues), and reviewing any security video footage, if available. All of these steps take time, and a TMT can assign responsibility based on each individual's expertise and role in the company. Keeping in close communication is important, and once again the actions are helpful in

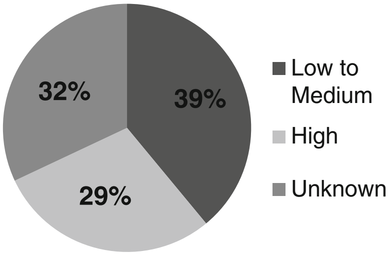

Figure 2: Initial level of threat assessed by 28 participating Threat Management Teams.

making sure this happens. For example, any interview should be *documented* so that information can be shared and a record kept; head of Security and company leaders should be *notified* of pertinent information as it becomes available; and, the case needs to be routinely *assessed* to determine if new information could lead to an increase or decrease in the level of threat.

The 28 TMTs in this tabletop exercise were asked to write a plan for the first actions to take. All of the teams (100 per cent) notified relevant parties and began their investigation. Only 18 per cent of the teams noted that they would document the investigation steps and none of the teams noted that they would offer consultation, such as to the unit or unit manager. In a real case, documentation and consultation are recommended at this stage. Using the tabletop scenario in conjunction with the Threat Management Assessment and Response Model can help TMTs remember all of the steps and to coordinate who does what. All of the teams (100 per cent) listed investigative steps in their next actions. Although this scenario is in the investigation phase, 18 per cent of the teams noted that they would take some intervention or referral steps, which included providing resources to the threatened employee and assurance to the unit. These steps would be helpful to ensure the unit that the issue was being addressed and demonstrate how many different activities can be conducted at the same time.

At this point in the tabletop scenario, the facilitator had each TMT review their written plan and compare the steps to other TMTs results. All of the 28 TMTs did a good job in identifying the next steps; however, the combined list was far more comprehensive than individual plans. TMTs working together in this type of environment (tabletop exercises) will create more comprehensive plans by learning from each other, and teams that have practiced developing plans will be more efficient in implementing their plans.

This example is a very simplified version of how the Threat Management Assessment and Response Model and a tabletop scenario training exercise can be used to train TMTs to respond to threatening behavior, threats and acts of violence in the workforce. In the training, the model and the tabletop scenario helped achieve the following:

- TMT members learned the different types of skills and resources that each member brought to the discussion. Following the training, participants reported increased confidence in carrying out their workplace violence prevention role. Discussion with the TMT led to a broader range of actions than individuals identified on their own. When the team made decisions together, a higher percentage of the four actions were completed at each phase
- Multiple phases could be implemented at the same time. For example, while the case is being investigated an intervention could still be implemented during the investigation stage (for example, safety plan for victim, discussion with unit).

At the conclusion of the tabletop exercise, the participants were asked about their experiences with the training. On a scale of 1–6, with 6 indicating strongly agree, the average response to the question ‘Training in this exercise increased my knowledge’ was 5.27. Furthermore, the exercise was very effective in increasing confidence of the participants in responding to workplace violence incidents. The highest gain in confidence, with a gain of more than 18 per cent, was in knowing the different roles and contributions of the various team members (Table 1).

Table 1: Changes in participant confidence in threat management activities, pre- and post- training

Role in the threat management process (ordered from highest to lowest pre-test confidence)	*Confidence on a scale of 1 (not very confident) and 10 (very confident)*		*Percent increase in confidence*[a]
	Average (range) pre-test	*post test*	
Making appropriate referrals for information and services	7.72 (2–10)	8.45 (3–10)	9.5
Documenting the appropriate information, in the appropriate place, during a threat management response	7.23 (2–10)	8.22 (5–10)	13.7
Conducting the appropriate follow-up during the final phases of the threat response	7.23 (2–10)	8.37 (5–10)	15.8
Acting quickly when a threat response is initiated	7.13 (2–10)	8.22 (5–10)	15.3
Gathering the pertinent data and information needed to identify and respond to threats	7.09 (4–10)	8.18 (5–10)	15.4
Communicating the appropriate information to the appropriate parties during threat identification and response	7.03 (2–10)	8.18 (5–10)	16.4
Knowing the roles of the other team members in the threat management process	6.95 (1–10)	8.05 (5–10)	18.8
Playing my role in the threat management process	6.86 (1–10)	7.99 (4–10)	16.5

[a] All items had a statistically significant increase in confidence ($P<0.05$).

Conclusion

The use of a multi-disciplinary team to assess and intervene in threatening behaviors, threats and acts of violence within organizations is not a new concept (Rugala and Isaacs, 2004; ASIS, 2011 and so on). However, little data or research is available to gauge the effectiveness of these teams or to help identify the optimal approaches to train and implement team activities. As illustrated by the case example in this article, and research conducted with the TMTs of the large multinational company, the use of tabletop scenario exercises can help teams practice the phases and actions that produce a coordinated response to threatening behavior, threats and acts of violence in the workplace (Peek-Asa *et al*, 2013). The goal of the team is bringing multiple viewpoints and areas of expertise within the company to assist in assessing, investigating, responding to, monitoring and mitigating cases in a coordinated manner that follows company policies.

Acknowledgements

This work was funded by the National Institute for Occupational Safety and Health (R21 OH009492).

References

Alterman, T., Luckhaupt, S.E., Dahlhamer, J.M., Ward, B.W. and Calvert, G.M. (2013) Job insecurity, work-family imbalance, and hostile work environment: Prevalence data from the 2010 national health interview survey. *American Journal of Industrial Medicine* 56(6): 660–669.

American Society for Industrial Security/Society for Human Resource Management (ASIS/SHRM). (2011) *Workplace Violence Prevention and Intervention*. Alexandria, VA: ASIS/SHRM.

Atack, L., Bull, E., Dryden, T., Maher, J. and Rocchi, M. (2012) An evaluation of learner perception of competency and satisfaction with tree models of an interdisciplinary survey capacity course. *Journal of Allied Health* 41(3): 106–112.

Borum, R., Fein, R., Vossekuil, B. and Berglund, J. (1999) Threat assessment: Defining an approach to assessing risk for targeted violence. *Mental Health Law & Policy Faculty Publications*. Paper 146. http://scholarcommons.usf.edu/mhlp_facpub/146.

Bureau of Labor Statistics. (2006) Survey of Workplace Violence Prevention. Washington DC: US Department of Labor. Report no. USDL 06-1860.

Bureau of Labor Statistics. (2013) National Census of Fatal Occupational Injuries and Illnesses, 2012. Washington DC: US Department of Labor. Report number: USDL-13-1699.

Chi, C., Chao, W., Chuang, C., Tsai, M. and Tsai, L. (2001) Emergency medical technicians' disaster training by tabletop exercise. *Am J Emerg Med* 19: 433–436.

Drew, S. (2005) Reducing enterprise risk with effective threat management. *Information Security Journal: A Global Perspective* 13(6): 37–42.

Department of Homeland Security. Office of Domestic Preparedness. Homeland Security Exercise and Evaluation Program. (October 2003). Volume II: Exercise Evaluation and Improvement. NCJ 202198. Washington, D.C. http://www.ojp.gov/odp/docs/HSEEPv2.pdf, accessed December 2007.

Federal Emergency Management Agency. Emergency Management Institute. Department of Homeland Security. (March 2003). Simulation Exercise Design. Independent Study IS139. http://www.training.fema.gov/emiweb/IS/is139lst.asp, accessed 3 April 2015.

Gillespie, G.L., Gates, D.M. and Mentzel, T. (2012) An educational program to prevent, manage, and recover from workplace violence. *Advanced Emergency Nursing Journal* 34(4): 325–332.

Harrell, E. (2011) Workplace Violence, 1993–2009. Washington DC: U.S. Department of Justice, Bureau of Justice Statistics. Report no. NCJ 233231.

Lyncheski, J.E. and Hardy, W.S. (2001) Workplace violence: Practical advice for a problem with dire legal consequences. *Health Care Law Monograph*, May: 17–25.

Meloy, J.R. and Hoffmann, J. (eds.) (2013) *International Handbook of Threat Assessment*. Oxford: Oxford University Press, pp. 3–9.

Peek-Asa, C., Casteel, C., Rugala, E., Romanoa, S. and Ramirez, M. (2013) Workplace violence investigations and activation of the threat management team in a multinational corporation. *Journal of Occupational and Environmental Medicine* 75(5): 870–876.

Pinkerton Consulting and Investigations. (2002) *Fortune 1000 Top Security Threats Survey*. New York: Pinkerton Consulting and Investigations.

Rugala, E. and Isaacs, A. (2004) *Workplace Violence: Issues in Response*. Leesburg, VA: Federal Bureau of Investigation, National Center for the Analysis of Violent Crime. http://Fbi.gov.

Securitas. (2014) Top security threats and management issues facing corporate America, http://www.securitas.com/Global/United%20States/2012%20Top%20Security%20Threats.pdf, accessed 23 March 2014.

University of Iowa Injury Prevention Research Center. (2001) Workplace Violence: Report to the Nation. Iowa City, IA: The University of Iowa. 17551/1-01.

White, S. (2013) Workplace targeted violence. In: J.R. Meloy and J. Hoffmann (eds.) *International Handbook of Threat Assessment*. Oxford: Oxford University Press, pp. 83–107.

Zapf, D., Escartin, J., Einarsen, S., Hoel, H. and Vartia, M. (2011) Empirical findings on prevalence and risk groups of bullying in the workplace. In: S. Einarsen, H. Hoel, D. Zapf and C.L. Cooper (eds.) *Bullying and Harassment in the Workplace: Developments in Theory, Research and Practice*. 2nd edn. Boca Raton, FL: CRC Press/Taylor & Francis Group, pp. 75–87.