When an organisation considers duty of care in high risk environments it automatically considers security practice. It thinks through the risks in the environment and how it mitigates those risks to provide duty of care to its employees. This is partly because the most demonstrable gaps in duty of care – and those which have resulted in the most lawsuits – tend to stem from security incidences. This can mean that duty of care can be unhelpfully associated only with security practice. If security practices are robust enough, the reasoning goes, then duty of care is demonstrated. The result is that duty of care is frequently 'assigned' to security managers as something they need to demonstrate through security policies and practices.

Unfortunately, in my experience, this assignment is not often accompanied by a definition, explanation or even training on duty of care. This leaves security managers responsible for a vague concept that, like the horizon, can be chased but never reached. Security managers operate with this looming sense that they might, or might not, be adequately contributing to duty of care and they'll only know if there is a failure for which they'll be held accountable.

Part of this issue is because duty of care is presented as a product rather than a concept. Duty of care is viewed by many as a checklist for a couple people within the organisation – usually the human resources and security departments - rather than an organisation-wide responsibility to which each department contributes. It is 'assigned' to certain people rather than being viewed holistically as a concept to which every employee has a responsibility and from which every employee derives care.

So, what is duty of care?

Duty of Care is most accurately described as a social contract – a combination of activities, actions, documents, policies, procedures, and practices which *indicate* that the organisation is attempting to keep people safe and inform them of any harm they might face. Security practice *is not* duty of care. Security practice *indicates* duty of care. This is a small but essential difference. Even if an organisation has every security policy and procedure considered best practice in a high risk environment they might still be found deficient in duty of care. Maybe they are hiring the wrong people for jobs, not paying them enough, not evaluating their performance, and requiring them to work too many long hours. All of these are outside the parameters of security management but are also indicative of duty of care.

From a legal perspective, duty of care is based on negligence. The question that a court would ask in a lawsuit is: Is there proof that the organisation could have provided reasonable care which would have kept their employees from harm? The answer to this will be determined by the court but it is likely that it will – if the case is related to a security incident – look at a number of factors. While each case will vary according to

the location of the incident, organisation, and individual there are 10 ways that security managers can effectively contribute toward their organisation's duty of care.

10 ways to manage your duty of care with security management

1. In a legal case, organisations will be judged by a community standard. This means it will be judged based on what other organisations were doing in that same environment and any common standards that had been adopted formally and informally. Security managers should not operate in isolation. They should be in regular contact with other organisations and understand what they are doing and why.

2. Have comprehensive security policies, training, adequate mitigation measures for each threat. Make sure that recording incidents (including near misses) any organisational learning from these are part of this.

3. Communicate with staff and ensure that they are **aware** of all the security information.

4. Conduct risk assessments and update them making sure they are up to date and specific to where the organisation operates.

5. Never compel staff to go to/stay in unsafe environments

6. Consider having a 'Duty of Care' document which states all security management actions taken to protect your staff.

7. Do not promise more than your organisation will or can deliver. The organisation will not benefit from promising staff policies or resources which it cannot always deliver.

8. Have appropriate insurances. In addition to purchasing any insurance required by law (vehicle, life, health, etc.) consider medevac, and compensation for staff members killed or injured.

9. Have a crisis management plan and operational crisis management team – usually at HQ and field level. And, more importantly, trial that plan. Run a simulation to help those on the crisis management team experience what a crisis will look like.

10. If the hostile environment's risks outweigh its benefits, be prepared to pull out of the environment if necessary.

Organisations which take these 10 aspects of security practice seriously will be well on their way toward providing the security aspect of duty of care to their employees.

Kelsey Hoppe, Organisational Development & Security Consultant
kelseyhoppe@gmail.com