The Coconut Effect

Communication competence within risk communication

B.Umiker, Risk Management Consultant, Psychologist lic.phil. and Engineer

The coconut effect as a process risk of awareness

As soon as you board the packed jetplane for Hawaii you begin to dream of the white beaches of the remote island of Kauai with its almost untouched natural beauty. At last you can enjoy sun, sea, sand and swaying palm trees and forget about the stresses and strains of everyday life. Right? Wrong! As soon as you take your first stroll along the paradise-like beach, you find a barrier blocking your way to the shady grove of majestic palm trees. In your relaxed holiday mood you defiantly clear the offending hurdle in one fell leap, only to pull up short at the first palm when confronted with an annoying sign declaring "No Trespassing".

"Everywhere the same idiotic bans and restrictions,", you think to yourself. "There's no freedom even in paradise!" A little annoyed but spurred on by your holiday-induced spirit of adventure, you ignore the unmistakable message and continue with a slight inner unease. But on the very next palm tree you come across another sign which warns, "Falling coconuts, keep out!"

Abruptly you come to a halt. With an anxious glance upwards at the dizzying height of the nearest treetop you wonder now if danger lurks in the form of a skull-breaking coconut ...
It is at this moment you become aware that you have entered a hazardous situation, and realise that the barrier as well as the "No Trespassing" sign are there for a real purpose: to protect you from danger.

What can we learn from this "coconut effect"?

∞ In order for any communication of risk to trigger the appropriate response, the risk must be recognised *and,* moreover, subjectively accepted.

∞ Hence the key tasks of security communications include not only issuing instructions on conduct and the implementation of associated measures, but also preparing the ground to ensure an effective awareness of risk, in order to ensure the correct response in line with security regulations.

∞ The struggle between the principle of pleasure (lust) and the principle of security is interesting from a psychological standpoint. In 1971 psychoanalyst H. Argelander[1] went so far as to place the security principle on an equal footing with the pleasure principle postulated by Sigmund Freud.

∞ A full risk awareness is only achieved if a person is clearly, unmistakably and comprehensively informed of the present dangers and the associated potential threats (information in the sense of practical, graphic facts).

So risk awareness is a necessary precondition and an integral component of risk communications. No general risk communications or risk dialog can be successfully achieved without the process of risk awareness in the above sense.

Why is risk communication necessary?

According to A. H. Maslow and others, Man's elementary need for security is expressed in the striving for safety and stability, uncomplicated and secure relationships, protection, freedom from anxiety etc. In its current form it is also identifiable nowadays as the need for a secure job, a safe place for of money in the bank and all types of insurances; as resistance to change; and as a tendency to assume world views that permit a safe lifestyle. Under the conditions of modern industrialised countries the collective need for security primarily manifests itself only in the event of spectacular crises and catastrophes (c.f. B. Umiker[2]).

Over the past few decades a large number of minor-to-medium sized upsets as well as several large-scale genuine disasters have increased the public's awareness of risk. But globalisation and deregulation of markets, structural and economic problems as well the very real threat of job losses have pushed issues of risk off the front pages. Nevertheless, the elements of risk have by no means disappeared. On the contrary: in addition to offering major opportunities, today's rapidly-changing technologies and global changes also entail risks which to some extent have not yet been recognised or are being studiously ignored. For example:

∞ One of the risks of globalisation is that productions or test series which are judged by the industrialised world to be too dangerous or critical are palmed off on developing countries with less restrictive laws. Production facilities are often set up in such countries without even a nod to the minimum safety standards, usually

1

2

for cost reasons. The disastrous accident in Bophal, India, involving thousands of victims, is a dramatic and tragic example of the consequences of such actions.

∞ Another critical development proves the necessity for constant vigilance and deserves closer scrutiny. Recently, in the wake of deregulation, many companies have slavishly followed modern management theories that declare the virtues of "lean production" and "shareholder value", and have trimmed down their workforce to a minimum. This, unfortunately, has led to more than just an increase in profits. Security and quality problems are increasingly coming to light, while operational and administrative processes are deteriorating due to a rise in the incidence of "human error". This risk potential is set to grow substantially within the near future.

Man's high need for security and the potential hazards to which he is exposed demand a comprehensive and open communication of all the risks an absolute essential.

Generally speaking, risk communication can be divided into three elements:

∞ the communication of messages or the exchange of information on security-related subjects, so-called information objects (the syntactic components of communications),

∞ their meaning for the recipient in the sense of safety-related facts (semantics)

∞ and - most notably - their ability to induce security-conscious behaviour (pragmatics).

Normally they occur as verbal (oral or written) and non-verbal interactions and as an understanding between two or more individuals or organisations whose main concern is security.

Wherever risk communications are required - in the prevention or fighting of fire, flood, accident, crime, espionage, computer system crashes etc. - it is of utmost importance that the message is communicated as the situation demands. Otherwise we have failed to fulfil the objectives and purpose of risk communications (see Fig. 1).

The purpose and objective of risk communication
(non-exclusive list)

1. To register and address people's need for security.
2. To create risk awareness for as yet unknown or undetected risks.
3. To draw up general rules and codes of conduct in respect of risks and security and to promote their acceptance.
4. To create functioning security-compliant information channels in order to communicate security-related information unmistakably to all persons who require it.
5. To ensure a Corporate climate and culture that encourages the appropriate conduct and caution in respect of risks.
6. To create within the organisation structures and regulations that meet security-related needs and requirements.
7. To enable a dialectical communication of divergent opinions between various interest groups in respect of risks and security.
8. To enable a risk dialogue within the organisation and with the outside world.
9. To enable an ongoing, process-led adaptation of security-related conduct, structures, facilities, regulations etc. at a conceptual and operational level.

Figure 1

These objectives additionally demonstrate that risk communications essentially takes place on two different levels:

∞ <u>On an abstract, conceptual level</u>

Here the task is to present for discussion, develop, test and introduce the necessary concepts, methods and measures to address recognised dangers and the associated potential threats. This should be done within the framework of a process-based, usually project-oriented procedure, remembering also to create the requisite information channels.

Typical results of such communicative processes include laws and rules (e.g. the government's ordnance governing civil disturbance), risk management concepts for high-risk production operations and factories[3], implementation concepts for emergency resources (fire-fighting service, police, ambulance), accident prevention measures, alarm and evacuation plans, the (ergonomic) design of signs drawing attention to bans, dangers and warnings, data protection, access authorisation and encryption concepts for IT and networks, IT emergency planning[4], insurance concepts for minimising a company's financial risk potential, etc.

∞ On an operational, implementational level

We are all confronted daily with the operational aspects of risk communications, mostly without recognising them as such.

Many security concepts have a direct impact by communicating risk information themselves . Examples include road traffic signs concerning bans, dangers and warnings, notices announcing the hazardous contents of containers and trucks, air traffic control, the police car siren, the barrier blocking our way to the palm grove.

Others serve as practical springboards for the concrete implementation of risk management concepts and of individual security measures. For example, intrusion alarms, telecommunications alarm systems, security password management systems for IT users, PIN code systems for credit and cheque cards, anti-theft systems in vehicles. Also included in this category are actual emergency communications, which must function seamlessly in a concrete emergency situation through the issuing of clear and simple commands, in some cases in a special emergency language (e.g. for firefighting services during a fire).

Several of these technical systems act as "autonomous" communicators, simultaneously serving as transmitter, interface and message (danger alert by a fire alarm system with integrated alarm transmission system).

However, high-level communication security is the prerequisite and decisive factor in the ability to achieve the above-named goals and to ensure successful risk communications at the conceptual and operational levels. Such security ensures that

∞ the messages communicated by the sender (signals) reach the recipient unaltered (physical level)

∞ the recipient understands the contents of the message as the sender intended (linguistic level)

∞ on a rational and emotional level, the recipient can perceive what the sender wanted to express (psychological level)

3

4

The example of risk dialogue, a component of risk communications as a whole, is used to present the following key communication principles.

Risk dialogue as a special form of risk communications

Despite a slowdown in the economy, we can no longer afford to dismiss the need for risk dialog when it comes to the implementation and operation of high-tech systems such as laboratories for microbiology and genetic engineering, nuclear plants and large-scale chemical installations that entail environmental risks. Increasingly this also applies to the world of rapidly-evolving information technologies and the global, unchecked networking of information on such media as the internet, where there is (as yet) practically no detectable awareness of the inherent social and socio-psychological risks.

Risk awareness must be created within the framework of multidisciplinary consultations and address all aspects of danger. This calls for open and frank discussions on the overall potential risk, carried out not only between enterprises but also between them and the various public interest groups, and as early as possible before the associated project proposals are implemented.

Risk management presupposes the elimination of misunderstandings or misinterpretations based on specific terminology used by different disciplines, in the interest of ensuring effective, universally understandable communications.

References:

[1]Argelander, H. — Ein Versuch zur Neuformulierung des primären Narzissmus
In: Psyche (31), 1977, 208 - 215

[2] Joffe, W.G. & Sandler, J. — Über einige begriffliche Probleme im Zusammenhang mit dem Studium narzistischer Störungen
In: Psyche (29), 1967, 152 - 165

[3] Umiker, B. — Psychologische Reflexionen über das Risk Management
Zürich: Walter Umiker + Co. AG, 1988

[4] Umiker, B., Bisang, P. — Wie lassen sich grosse Industriekatastrophen verhüten?
In: IO-Management-Zeitschrift (56), 1987, 15 - 22

[5] Umiker, B.; Peer, A.; u.a. — Warum braucht jedes Unternehmen ein Informatik-Notfallkonzept?
In: IO-Management-Zeitschrift (64), 1995

[6] Umiker, B, — Kommunikationssicherheit in der Sicherheits-kommunikation Vortrag an der ETH-Z für American Society for Industrial Security Juni 1997

Zürich,15.02.0216.02.02