What should consumers do? Well, certainly they should be aware of such attacks, and be generally cautious of anything that looks suspicious. Also they might like to consider anti-phishing software, which attempts to identify phishing content contained in Web site and e-mail software.

Other threats include those involving spyware (a piece of software that is installed surreptitiously on a PC and laptop to intercept or take partial control of the user's interaction with the computer, without the user's informed consent) and malware, which might interfere with the function of other software applications on the PC or laptop, in order to force users to visit a particular Web site.

ISO/IEC 27002 provides many other best practice controls to protect IT, which consumers should consider such as:

- Use of personal firewalls which helps to stop unauthorized access to a PC or laptop when connected to the Internet;
- Use of encryption to protect files stored on PCs and laptops to avoid anyone gaining unauthorized access reading the content of consumers files;
- Physical protection against the theft of IT, especially of mobile products such as laptops, mobile phones and personal data assistants, all of which become easy targets for thieves.

There are many products on the market, which would support the implementation of this best practice advice.

In summary, protecting consumers' information and IT is a combination of:

- Awareness of the risks involved;
- Doing something about these risks by applying best practice as provided in ISO/IEC 27001 (some examples of which are given above);
- Using some of the products available where they are necessary to support this best practice (not all best practice controls need to use technology). ■

Flood in Riga, Latvia (Photo: iStock)

Societal security – ISO tackles a new field for standards

by Dr. Stefan Tangen, Secretary of ISO/TC 223, Societal security

Many natural disasters, accidents and terrorist attacks in recent years have propelled the issue of crisis management to the top of the national agenda in many countries, such as the recent flooding in England. In order to meet the demands of emergency management, governments need to engage civil society organizations and the private sector to better prepare, respond to and recover from such crises.

The classical focus on national security will continue to expand in the future to address a broader range of concerns. This shift entails the ability of government, business and civil society to function in a crisis, during which critical infrastructures must be sustained, the democratic ability to govern must be maintained, and certain basic values are upheld. It is difficult under the pressure of a severe crisis to maintain all of these functions. Several security elements that traditionally were once separate are becoming integrated: procedures for peace and war merge, internal and external security are interlocked, and enhancing state security and providing citizen safety become blurred. These new elements bring about many implications. Among them are the concepts and tools that are needed to enhance security, citizen safety and crisis management capacity in an increasingly interdependent and borderless world. These transboundary challenges are not covered by the traditional concept of national civil defence.

Crisis management and emergency services

The first plenary meeting of ISO technical committee ISO/TC 223 was held in Stockholm, Sweden, in 2006, attended by 68 delegates from 30 countries.[1)] The meeting was chaired by Ambassador Krister Kumlin, Senior Adviser to the Swedish Emergency Management Agency.

1) ISO/TC 223 was first initiated in 2001 under the title *Civil defence.* After a period of non-activity, the secretariat was given to the Swedish Standards Institute (SIS) at the end of 2005 and its title changed to *Societal security.*

*Chair of ISO/TC 223, Ambassador **Krister Kumlin.***

The 2nd plenary meeting of ISO/TC 223 held in Bangkok, November 22-24, 2006.

Delegates agreed to focus their work on increasing crisis and emergency management through technical, management and operational approaches, as well as interoperability of emergency services. The standards developed by ISO/TC 223 will help provide protection from and facilitate emergency responses to risks from natural disasters, accidents and terrorist attacks that disrupt daily life, business operations and government services. The committee uses an all-hazards perspective covering the phases of emergency and crisis management before, during, and after a societal security incident.

The technical committee has continued to grow and more than 100 delegates are expected to attend the 4th plenary meeting, which will be held in The Hague, Netherlands, 14-16 November 2007.

Control, coordination and cooperation

At the moment, the committee has 29 participating members and 22 observing members and is organized in the following working groups (WG) and task group (TG):

- WG 1: *Framework standard on societal security management*;
- WG 2: *Terminology*;
- WG 3: *Command and control, coordination and cooperation*;
- TG 2: *Preparedness and continuity*.

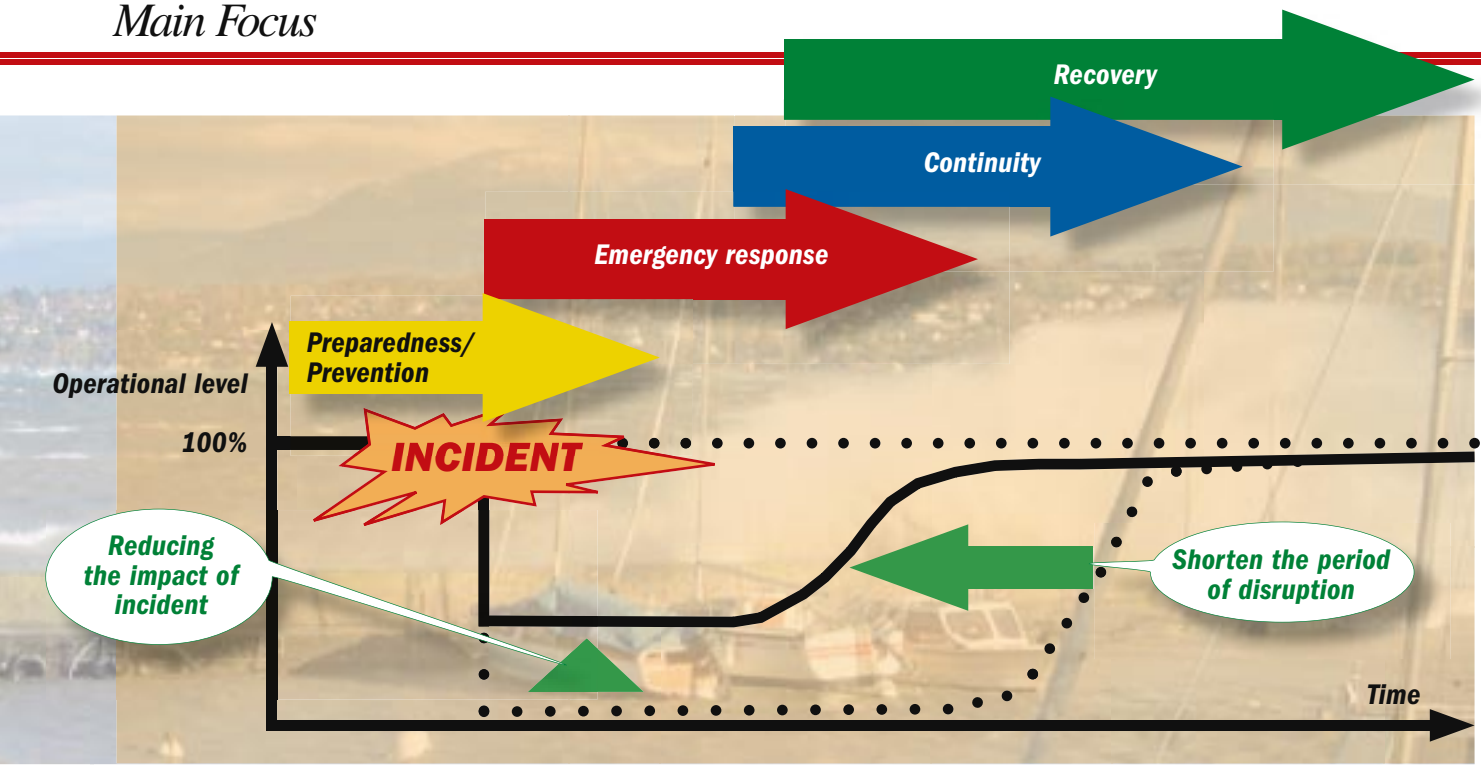
These groups are responsible for the development of several work items (the future ISO 22300 series):

- Essential information and data requirements for command and control;
- Inter/intra organizational warning procedures;
- Principles for command, control, coordination and cooperation in resolving incidents;
- Framework for standards;
- Vocabulary;
- Systems requirements for interoperability.

Many emergency situations take place in developing countries and their participation is therefore essential in the work of ISO/TC 223. For this reason, the

About the author

Dr. Stefan Tangen is the Secretary of ISO technical committee ISO/TC 223, *Societal security*, and a project manager at SIS, Swedish Standards Institute. He has previously been the Secretary of ISO/TC 184/SC 2, *Robots and robotic devices,* and has worked with numerous Swedish mirror committees. Before joining standardization, he worked as a senior researcher at the Royal Institute of Technology in Stockholm. Dr. Tangen holds a PhD degree in production engineering.



The concept of incident preparedness and operational continuity management.

committee established a developing country contact group in order to ensure that its work reflects the needs and experiences of developing countries. The concept of twinning is also an important part of the committee's work, with the United Kingdom and Trinidad and Tobago sharing the convenorship of WG 2. Similar arrangements are under preparation in the other working groups.

Guidelines for preparedness and continuity

The publication of ISO Publicly Available Specification ISO/PAS 22399, Societal security – Guidelines for incident preparedness and operational continuity management[2] will be based on five main contributions made to the ISO Workshop on Emergency Preparedness held in Florence, Italy, in April 2006, including parts of the US National Fire Protection Association (NFPA) standard NFPA 1600, Standard on Disaster Management and Business Continuity Programs, the British standard BS 25999-1, *Business Continuity Management* Part 1: Code of Practice (British Standards Institution), HB 221, *Business Continuity Management,* of Standards Australia, the standard from Standards Institution of Israel, INS 24001:2007, *Security and continuity management systems – Requirements and guidance for use*, and the work of the Japanese Industrial Standards Committee.

"The committee covers the phases of crisis management before, during, and after a societal security incident."

The publication of ISO/PAS 22399 guidelines will establish the process, principles and terminology of incident preparedness and operational continuity management (IPOCM) within the context of societal security. The purpose will be to provide a basis for developing and implementing emergency preparedness and operational continuity within an organization and to provide confidence during an emergency between organizations, communities and business. The guidelines will provide a tool to allow public or private organizations to consider their preparations to respond to disruptions to their operations in an emergency situation. It will enable them to manage and survive the incident and take appropriate action to help ensure the organization's continued viability. ISO/PAS 22399 will enable the organization to measure in a consistent and recognized manner its IPOCM incident preparedness and operational continuity management capability.

Interested parties and stakeholders require that organizations proactively prepare for potential incidents and disruptions, in order to avoid suspension of critical operations and services or if operations and services are disrupted that they resume operations and services as rapidly as required by those who depend on them. IPOCM is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for minimizing their effect.

The work of ISO/TC 223 will become increasingly important in the coming years to help organizations and communities deal with and recover from emergencies. It will allow them to develop procedures and systems, thus making them feel more prepared and confident to handle crisis situations when they arise. Preparedness and continuity are keys to saving lives and helping affected communities rebound when disaster strikes, thus giving them more resilience than those who are not prepared. ■

2) ISO/PAS 22399 is being prepared for publication and will be available in September 2007.