Responsible Care Security Code Guidance and Best Practice for the Implementation of the Code

Security management became increasingly important during the past ten years within the global business environment. Numerous regulatory and voluntarily initiatives have emerged to enhance the security of the private sector. In 2010, the Cefic National Association Board adopted the European Responsible Care Security Code as the basis for the inclusion of Security management into the national Responsible Care programmes in Europe.

This document is designed to assist companies in implementing the Responsible Care Security Code along seven management practices. A number of other guidance documents including risk assessment tools, checklists and best practice modules are available and can be used by companies. Those documents are listed in ANNEX 1.

1. Leadership Commitment

Senior leadership commitment to continuous improvement through policies, provision of sufficient and qualified resources and established accountability.

1.1. Emphasise security as a fundamental part of the overall management system and/or the Responsible Care program in form of e.g. a written policy or statement to all staff and partners.
1.2. Develop a job description for a person responsible for the company's security program and appoint a person based on the defined needs.
1.3. Define the internal security network and services especially if the company exists of more than one site or facility.
1.4. Take care of the job specific training and qualification for all staff dealing with security.
1.5. Provide the security function with sufficient resources and with direct reporting lines to the management.
1.6. Set and communicate security expectations and goals.

2. Risk Analysis

Periodical analysis of threats, vulnerabilities, likelihood and consequences using adequate methodologies.

2.1. Assess the most important assets for the company and for each relevant site e.g. research facilities, production plants, headquarters, central computer/computer rooms and infrastructure. Think about the possible impact triggered by theft, loss, damage, disruption, manipulation with malicious intent, rumours or espionage.

2.2. Evaluate the dependence on raw materials, telecommunication (phone, radio and data network), transport and utilities like energy.
2.3. Identify critical chemicals/products and processes whose theft, loss, manipulation or release caused by a malicious act could result in significant impacts for the company or the public e.g. tank farms, dangerous goods loading facilities, high pressure equipment, process control systems. Take into account any relevant assessments that the company has already performed.
2.4. Analyse the essential security threats for the company, the staff, the assets, the products and the knowhow. Know about the motivation and tactics of e.g. thieves, hackers, frustrated employees, organised crime, violent pressure groups, extremists and terrorists. Governmental and local security agencies should be asked to provide initial information and maintain a reporting system.
2.5. Make sure that a security analysis is a fundamental aspect of the overall business continuity planning and decisions on all capital expenditures and investments.
2.6. Determine what is acceptable and what is not

3. Implementation of Security Measures

Development and implementation of security measures commensurate with the risks.

3.1. Define the goals of a company specific security concept, based on a risk analysis and guided by the principle "Deter, Detect, Delay and Respond".
3.2. Conduct a security survey for the company or the site to assess the already existing security measures. For this purpose build a team consisting of management representatives and experts for security, process safety, infrastructure, IT, emergency response, logistics, human resources, etc. It is important to understand how technical, personnel and organisational means of security act together and help to secure other processes e.g. within the supply chain.
3.3. Analyse if there are any gaps between these measures and the risk and the goals defined before.
3.4. Close the gaps by putting additional or modified security measures into place, resulting into a comprehensive plan for site security which should cover all relevant categories.
3.5. Implement the plan and check that scheduled measures have been put in place and are working as desired, especially in case of significant modifications
3.6. Integrate security and information protection needs and requirements into site procedures, contracts and service level agreements, in an appropriate way and whenever necessary

See ANNEX 2 for good practices for items usually included in a security plan

4. Training, Guidance and Information

Training, guidance for, and information of employees, contractors, service providers and supply chain partners, as appropriate, to enhance security awareness.

4.1. Make sure that staff, contractors, suppliers and service provider are aware of, and respect the company's security rules and procedures. This information should be a fundamental part of the "day one" package for new employees and contactors but also for e.g. visitors, possibly in a shortened version.
4.2. Raise the general awareness for security and information protection by appropriate measures like presentations, workshops, training sessions, posters, flyers and any state-of-the-art communication technology or platforms.
4.3. Inform and train staff involved with critical assets or functions in more detail about the particular security and information protection threats caused not only by outsiders but also by insiders.

5. Communication, Dialogue and Information Exchange

Communications, dialogue and information exchange on appropriate security issues with stakeholders such as employees, contractors, communities, customers, suppliers, service providers and government officials and agencies, balanced with safeguards for sensitive information.

5.1. Establish means of communication, possibly making use of already existing ones within the company
- to inform employees, as appropriate, about current security threats and countermeasures, and
- to inform management, as appropriate, about lessons learned from security threats, incidents and investigations that have occurred.

5.2. Establish regular information exchange meetings with local/national law enforcement agencies and make sure that they will inform you immediately about upcoming threats.
5.3. Make sure that when there is a change in threat level, site security but also management and other relevant units are informed and will react as required or appropriate. Several threat level systems can exist that may have an impact on the company and these can include national and international systems.
5.4. Build or extend already existing networks within the industry for the exchange of security best practices and other relevant security information.

6. Response to Security Threats and Incidents

Evaluation, response, reporting and communication of security threats and security incidents, as appropriate, and corrective action for security incidents including "near misses".

6.1. Establish a reporting system for security issues or extend an already existing reporting process
6.2. Evaluate incidents without delay in order to reduce or to limit the impact.
6.3. Establish a Crisis Management/Emergency Response Organisation for handling major security incidents, whereby the use of existing teams is recommended.
6.4. Make sure to be able to rely on local or national law enforcement agencies which provides a 24/7 single point of contact.
6.5. Establish a "lessons-learned culture" for security issues inside the company and with others, as appropriate.

7. Audits, Verification and Continuous Improvement

The commitment to security calls on companies to seek continuous monitoring of all security processes.

7.1. Integrate security in the "management of change" processes.
7.2. Evaluate on a regular basis the number and severity of reported company internal security incidents and outside security incidents relevant for the chemical industry to keep the security system updated.
7.3. Make sure that the security processes and procedures are reviewed on a regular basis by internal or external experts.
7.4. Integrate security into the regular review system of the company e.g. Responsible Care.

ANNEX 1

References or other useful reading

1. **Leadership Commitment**

2. **Risk analysis**
   - IMPROVE: Vulnerability assessment methodology for chemical sites
     http://click-in.cefic.org/document/security-vulnerability-assessment-tool.aspx
     (via Cefic Click-in)

3. **Implementation of Security Measures**
   - EC Council Regulation (EC) No 881/2002 (OJ L 139, 29.5.2002, p. 9-22), which imposes a number of specific restrictive measures directed against suspected terrorists:
     http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:139:0009:0022:EN:PDF
     Note that the Annex, containing the list of persons and entities, gets amended frequently.

4. **Training, Guidance and Information**
   - Industry guidelines for the security of the transport of dangerous goods by road
     http://www.cefic.org/Documents/IndustrySupport/RC%20tools%20for%20SMEs/Document%20Tool%20Box/Security%20Guidelines%20of%20the%20transport%20of%20dangerous%20goods.pdf?epslanguage=en
   - e-Learning tool for the AEO (Authorised Economic Operator) legislation that aims at balancing increased security requirements with facilitations for compliant traders
     http://ec.europa.eu/taxation_customs/common/elearning/aeo/index_en.htm
   - Chemical security awareness training (requiring free of charge registration)
     http://www.dhs.gov/chemical-sector-training-and-resources

5. **Communications, Dialogue and Information Exchange**

6. **Response to security Threats and Incidents**

7. **Audits, Verification and Continuous Improvement**

Examples of existing security legislation and initiatives: Chapter 1.10 of RID/ADR/ADN, ISPS, C-TPAT, AEO, etc

ANNEX 2

Good practices for items included in a site security plan
(related to item 3. "Implementation of Security Measures)

a) Perimeter security: Fence, wall, gates, pedestrian entrances, turnstiles, barriers, doors and windows of buildings located directly at the fence-line must have a homogenous security level.

b) Locking devices: External gates, doors, windows and emergency exits must be secured with sufficient locking devices. Keys have to be checked on a regular basis.

c) Gate areas: Sufficient parking space for private vehicles and sufficient waiting and control areas for trucks and contractors must be present. The strict separation of external and internal territory is a must.

d) Lighting: Adequate illumination for gate areas, site perimeter, loading facilities and security control points should be installed.

e) Patrols: Depending on the size and the complexity of a facility, random patrols by security officers to check the site perimeter and also critical assets could be useful.

f) Video surveillance and sensors: The use of CCTV (Closed Circuit Television), fence detection, etc depends very much on the risk and the needs of a chemical facility. If necessary those systems need to be designed by experts and must be adapted to the technical and organisational capability of the internal or external security organisation.

g) Access control: All people (staff, contractors, visitors, guests, truck drivers, service providers, consultants, etc) have to be checked before getting access. Company badges for staff could be used for identification. All other people have to present a valid official document with a photograph like a passport. The host has to be contacted before access is granted or should pick up the person at the gate or entrance. In case of drivers, service providers, etc the relevant internal unit has to be contacted for verification. Company badges should be visibly displayed permanently by each person on site or within the facility. Huge and complex sites should have a sound system for denying access to (parts of) the site to unauthorised persons.

h) Access control technology: Automated access control systems, in combination with physical barriers, assist or can replace the guard function. In addition to the need for an up-to-date technology, the administration of such access control systems is very important: the administrator must be very reliable and qualified but it must be ensured that the data flow (in both directions) between the human resources data base, the badge producing system and the access control system, results in nearly instantaneous synchronisation.

i) Additional layers of protection: If the risk assessment identifies critical assets it must be checked whether additional protection with intrusion alarm systems, CCTV or other sensors might be necessary. Note that also physical and other security measures are essential for those assets.

j) Security operations: Tasks and duties of the site security function should be defined and documented. Security officers need to have job related education, training and qualification. Security incidents (near misses) and findings during patrolling etc. should be reported. Make sure that the security officers have all the information, training and equipment they need for alarm verification/response and patrolling.

k) Controls and inspections: Sufficient inspections of arriving and departing trucks, cars, containers, railcars, mail, etc should be established at the gates and/or at the relevant places inside like loading and unloading facilities, mail room, packaging etc. Use should be made of adequate inspection checklists specifically for trucks and containers; the U.S. C-TPAT program offers some good examples. Trucks and containers shall be secured by seals which are accepted for international transport.

l) Personnel security: Based on national legislation companies should have a process in place to screen employees and candidates for employment at the start of the employment and at regular intervals thereafter. Comply with the European Council Regulation No 881/2002 which imposes a number of specific restrictive measures directed against suspected terrorists.

m) Trade control: Security is a horizontal function within an organisation. It must therefore be ensured that, by formation and training, the security aspects in the areas of e.g. the Chemical Weapon Convention, explosive precursors, drugs and drug precursors are known and complied with by logistics, marketing and sales and all other involved units and staff of the company. Measures relate mainly to customer credibility checks, end-user declarations and the selection of reliable service providers such as e.g. forwarders.

n) Information Protection: In addition to the intellectual property aspect of information protection activities, it is also important to protect any other company information and systems against unauthorised access, misuse and manipulation. Therefore strong access procedures and controls to systems and applications are essential although the "need to know" principle must be taken into consideration. Business partners which duly need access to those systems and applications, have to be informed and trained but also monitored.

o) Maintenance: All security installations and systems must be regularly checked and maintained in working condition. All system failures and damages must be reported and repaired without any unacceptable delay.

p) Regulations: If the company is affected by laws and regulations with security aspects included (e.g. transport regulations for dangerous goods such as ADR, RID, ADN) these additional specific requirements need to be included within the overall security plan of the company or the site. Some security measures such as video monitoring may be limited or affected by national legal regulations.

June 2013