

CS&A

INTERNATIONAL RISK, CRISIS & BUSINESS CONTINUITY MANAGEMENT

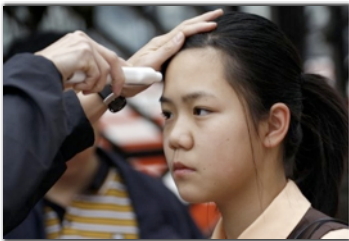
NEWSLETTER

SUMMER 2009 - ISSUE 4

In This Issue

Crisiscom© Helps Energy Services Company Communicate During Swine Flu Outbreak in Mexico	1
International Schools Move to Enhance Crisis Preparedness	1
Contingency Planning is Good for Business, by Ruud Kloppenburg	2
Upcoming Seminars and Courses	4
Hong Kong - based Team of Associates Expands	4
Hot off the Press	4

International Schools Move to Enhance Crisis Preparedness



H1N1-Temperature check in Hong Kong schools

Responding to the ever-increasing risk environment, international schools are moving to enhance their crisis preparedness and resilience. In Asia, Hong Kong's international schools recently took the lead by organizing a two-day crisis management seminar bringing together senior educators from across the territory's leading international schools, as well as representatives from local law enforcement and consular staff. Hosted by Hong Kong International School (HKIS), the seminar was conducted by CS&A, and generated enhanced cooperation among the institutions and their stakeholders to be better prepared to prevent and respond to crises more effectively.

Article continues on page 4 →

Crisiscom© Helps Energy Services Company Communicate During Swine Flu Outbreak in Mexico

Tenaris, a leading supplier of tubes and related services for the world's energy industry has been implementing CS&A's virtual crisis management tool Crisiscom© across its organization, and used it "live" to communicate during the recent swine flu outbreak in Mexico. The system, which enables real-time and virtual crisis management and communication was particularly beneficial to the teams during this difficult period when the Mexican government took severe measures in order to contain the outbreak. Crisiscom©'s navigation-friendly, real-time log, information sharing facilities and reliability features were reconfirmed in this context. The system, designed and developed by CS&A, is ideally suited to maintain critical information exchange and coordination among teams operating globally and during crises, especially protracted ones such as pandemics.

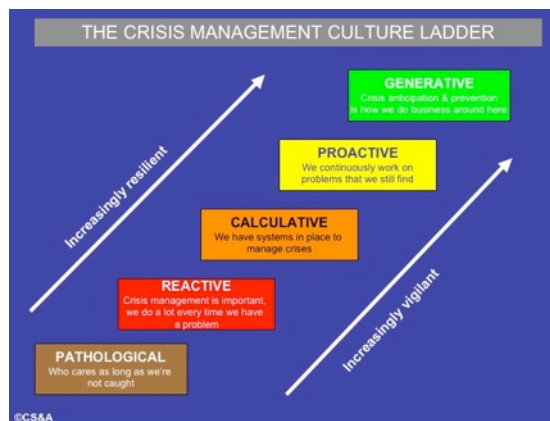
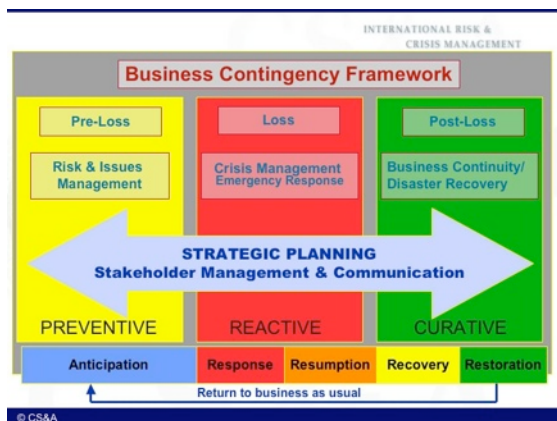
For a demonstration of Crisiscom©, please contact dirk.lenaerts@csa-crisis.com

Mexico City: A street vendor takes advantage of the outbreak by selling face mask, Mario Guzman/EPA



Contingency Planning is Good for Business

To help clients enhance their crisis anticipation, prevention, mitigation and recovery capability, CS&A applies a business contingency framework, which distinguishes and integrates three principal phases, namely pre-loss, loss and post-loss. This framework (see Graph 1) can be applied effectively across all corporate management functions, including security, HSE, financial planning, communication, IT, HR among others, and it is designed to enhance an organization's overall resilience and reliability. Following such a model can help organizations climb the crisis management culture ladder (see Graph 2) to attain a generative level of preparedness as illustrated below.



From a security management point of view, during the pre-loss phases all efforts are focused on the prevention of security incidents and emergencies by developing and implementing mutually supporting arrangements, called the security management system. This concept is illustrated in Graph 3 below:



Costs of calamities are usually high. Not just the direct and visible costs related to the material damage but more so the indirect, invisible costs resulting from loss of reputation, market share, customer's and shareholders' confidence and business continuity. This acknowledgement justifies the introduction of a professional security loss prevention programme.

To be successful in minimising the likelihood of calamities, it is important that organisations adopt security as a key business function and adhere to a number of security policies, principles and practices, the most essential of which are listed below.

A strategy that defines the company's intention, objectives and direction regarding security, guided by international security standards and compliance with legal, statutory and other regulatory requirements. Such a strategy makes a security system authoritative and enables the indispensable cooperation with and support by the national authorities of law and order.

Business organisations are used to assess and take risks. Without risks there are no opportunities. Therefore, organisations should equally use a risk management approach for their security, which is based on assessment of the risks and subsequent application of proportional counter-measures. This guarantees cost-effective security and avoids overreaction. Any other security approach, e.g. consequence-driven, rule-based or triggered by incidents alienates security from the general business, delays decisions, generates unnecessary costs and may even create a false sense of security.

Security in an organisation should be managed by a Chief Security Officer (CSO), who is familiar with the business organisation and its operations and has a solid support base amongst management and staff. Therefore, it is worth considering recruiting a CSO from the business and training him in security rather than looking for an officer from the intelligence, police or military services. In a large and complex organisation, an externally recruited individual will need at least three to four years before he or she will begin to understand the rules of the game in the business organisation and its internal politics. This familiarisation process may be detrimental to the security operations and credibility of the security organisation.

An important condition to maintaining good business reputation and continuity is the integrity of operations. This business value is best described as the intended use and complete functioning of all operational assets, including equipment, installations and sites. The biggest threats here include dishonest and disgruntled staff and unreliable third parties involved in malicious and criminal activities. Organisations should have control mechanisms in place to regularly verify/validate the integrity of their employees and the reliability of contractors, suppliers and other third parties. This integrity process will meet strong resistance in cultures where trust in people is indisputable.

Despite good protective measures, security incidents and emergencies will occur. Incidents are almost daily events that cause little or no damage and are dealt with by line management as part of routine operations. Reporting, recording and investigating procedures will control incidents at an early stage and prevent them from escalating to emergencies.

Security emergencies, however, are major and potentially high consequence events that should be countered/mitigated in an organised and responsible way. During the pre-loss phase, the likelihood of calamities should be assessed, plans to manage them developed and emergency response teams organised, trained and exercised. Winston Churchill's famous saying "failing to plan is planning to fail" is ever so relevant.

Finally, organisations should establish appropriate measurements for security performance. The main objective of this measurement process is simply to confirm that risks and measures are still in balance. Measurement tools include self and independent assessments and formal audits. Benchmarking is a good instrument to compare the security quality and effectiveness with other organisations. However, the most effective tool to ensure that security remains in good shape is introduction of an assurance process throughout the organisation, whereby business managers are required to confirm compliance with the security management system via an annual questionnaire. This enables the organisation to detect deficiencies in the security concept at an early stage and take corrective actions.

As said earlier, good prevention does not prevent calamities from happening. However, they definitely help minimise their likelihood and maximise the quality and effectiveness of the response and recovery processes.



Based in Amsterdam, The Netherlands, Ruud Kloppenburg, is an expert in all aspects of international security and an adviser to CS&A International Risk, Crisis and Business Continuity. For more information on this article or its author, please contact: caroline.sapriel@csa-crisis.com

Continued from page 1

International Schools Move to Enhance Crisis Preparedness

Although Hong Kong itself is not viewed as a particularly high-risk environment, the threat of pandemic and extreme climatic events are some of the factors causing uncertainties and concerns among parents, students and teachers. Overall, there has been increased incidence of criminal and violent events at schools such as hostage taking and shootings. Facing such threats as well as the widespread use and misuse of the internet and new media among youth, there is a concerted effort to enhance awareness and communication among stakeholders, so that schools are better prepared to respond to crises effectively.

“There is a tremendous amount of value derived from coming together as colleagues to discuss these types of issues and learn new methods of dealing with crises at our institutions. The insight that CS&A brought to the table relating to communication and family issues was invaluable”, said Richard Mueller, Head of School, HKIS.

During the seminar, topics such as security, victim and next-of-kin assistance, as well as media and stakeholder communications were introduced, and practiced by participants through desktop exercises.

The business community has a vested interest in ensuring that schools are well prepared to protect students in the event of crises. This is quickly becoming a focus of business continuity planning: when schools are threatened by major events, it can have an immediate and considerable impact on our business because our executives will want to be there to look after their children, a senior international banker recently told CS&A.

Judging from the level of interest received, CS&A are planning to repeat this seminar in Hong Kong in the fall and run similar events elsewhere in Asia and in leading cities in Europe where there are important international school communities.

For more information on this seminar, please contact: caroline.sapriel@csa-crisis.com

Upcoming Seminars and Courses

Kuala Lumpur and Hong Kong August 13-14 and 17-18, 2009

Caroline Sapriel, CS&A Managing Director leads two Crisis Communication Seminars organised by Singapore-based, UNI Strategic, leaders in business-to-business intelligence and external and in-house training programs, and regional conferences. For details and registration, please refer to:

Kuala Lumpur

http://www.unistrategic.com/index.php/component?option=com_eventlist/Itemid,4/did,274/func,details/

Hong Kong

http://www.unistrategic.com/index.php/component?option=com_eventlist/Itemid,4/did,275/func,details/

London, October 13-14, 2009

Steel Business Briefing, the steel industry’s leading trade publication, is teaming up with CS&A to organise a two-day seminar on Crisis Management Planning, which will focus on crisis anticipation, detection, mitigation and recovery.

For details and registration, please contact : caroline.sapriel@csa-crisis.com

Agnes Hui Joins CS&A’s Hong Kong-based Team of Associates

See her full biography on: <http://www.csa-crisis.com>

In the News

Articles by Lina Kolesnikova, Brussels-based CS&A Associate

1. Joint Front: Counter-terrorism struggle at CIS

(Journal of International Security/May 2009)

2. European Disaster Relief Force: Is it the right time to move?

(Crisis Response Journal, Volume 5, issue 3, June 2009)

3. Building Terrorism Resistant Communities. Together Against Terrorism.

Volume 55 NATO Science for Peace and Security Series - E: Human and Societal Dynamics. Chapter: Achieving resilience in communities: lessons learned from terrorist attacks.

For more information on these articles, please contact caroline.sapriel@csa-crisis.com