SOLUTIONS TO REDUCE SECURITY INCIDENTS AND LESSONS LEARNED

Mike ZEEGERS

Abstract

Protecting a nation and Critical Infrastructure against terrorism and other malicious acts is one of the main tasks of this century. A country and its Critical Infrastructure must be protected and able to resist and swiftly recover from all hazards. Proactive and harmonized efforts are essential in strengthening and preserving secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital for the Nation's safety, prosperity, and well-being. There are various ways of achieving such a goal, including Incident Management System and its key factors, Security Risk Management System, and Security Risk Assessment. Absence of a formal Security Risk Management System which includes a formal Risk Assessment may be viewed as indicative of a lack of due diligence and effective risk management.

Key words

Critical Infrastructure, Safety, Security Risk Management System, Security Risk Assessment, Risk analysis.

1 Introduction

Security incidents and incident management is highly underestimated, hence profitable for criminals.

Understanding the incident management system requires a holistic approach by following security strategy and policy of the organisation, e.g. security values via missions, visions, requirements, guidelines, and multi-year planning.

This approach results in a cross security risk approach, between Corporate Standards and development of a Security Management System.

Key factors in the Security Management System are Security Policy stated and signed by the Board of Directors, Security Risk Assessment, Implementation and Operations, Checking and Corrective Actions, and Management Review and Improvement, all done in relation to the Plan-Do-Act-Check circle. In doing so, it goes beyond a mere statistical analysis of security incidents and conducting a threat assessment, it provides a strategic analysis of one of the most important part of the Security Management System. Furthermore, it includes analyses of selected threats, reviews of policy, security counter measures, risk matrix, etc. Undoubtedly this presents a lot of effort. But security incidents have enormous economic impacts on organisations. We need to improve our ability to identify these impacts on both individual organisations and on a European level. This is the reason why future work should aim at understanding and analysing how Security Risk Management Systems can be introduced as an integrated part of the business strategies for all organisations.

2 Fields of Security

- **Critical Infrastructure**

Protecting Critical Infrastructure against terrorism and other malicious acts is one of the major challenges of the 21st century. To assist this, the European Commission has founded

many projects during the past years. The European Commission has been working with a number of European Security Specialists to develop common easily usable tools, and designed a Security Risk Management System for each part of an industry.

- **The Islamic State threats**

The Islamic State (IS), also widely known as ISIS and ISIL, is attempting fulfil its promise to attack nations who oppose them. ISIS militants pose a "greater threat" to the world security "than we've seen before" and are more dangerous than al Qaida.

This threat cannot be solved simply by dealing with perceived grievances over the western foreign policy. Nor can it be dealt with by addressing poverty, dictatorship or instability in the region - as important as these things are. "The root cause of this threat to our security is quite clear. It is a poisonous ideology of Islamist extremism that is condemned by all faiths and faith leaders.

Underlining the threat faced by countries in the West: "There's no doubt in my mind that IS is targeting all of us ... in Europe". Nevertheless we should be prepared and particularity high profile organisations in Europe. [1]

- **Security Intelligence**

"Security Intelligence is the real-time collection, normalization, and analysis of the data generated by users, applications and infrastructure that impacts the security and risk posture of an organisation. The goal of Security Intelligence is to provide actionable and comprehensive insight that reduces risk and operational effort for any size organization." [2]

Security Intelligence reduces security risks and gives operational effort to organisations and is an integrated part of the Security Risk Management System.

Through incident registration, security intelligence, policies and Security Risk Assessment we create the Security Risk Management System.

- **Key Requirements for Europe**

Many European States already have Critical Infrastructure Protection (CIP) programmes. The EC accepts that CIP is foremost a national responsibility however, trans-national dependencies and impacts require an EC approach. Therefore, proposals exist to identify and designate sites which are European Critical Infrastructure (ECI). Transport and energy sectors are designated as a priority. ECI designated sites will require a mixture of binding and non-binding measures including the establishment of an Operator Security Plan (OSP).

If an organisation is designated as ECI, binding measures on Member States and Operators essentially require establishment of an Operator Security Plan (OSP) which includes: [3]

- Identification of important assets.
- A Risk Analysis based on major threat scenarios, vulnerability of each identified asset and potential impacts. In short, a Security Risk or Vulnerability Assessment.
- Identification, selection and prioritisation of countermeasures and procedures.
- The designation of a Security Liaison Officer (SLO).

3 Security Risk Management System

A Security Risk Management System provides a framework for an organisation to assess, in a systematic manner, the security environment in which it operates, to determine if adequate preventive, responsive, and contingency measures are in place, to implement and maintain security measures, and to review the ongoing effectiveness of the system, in line with international standards and guidelines.

Security Risk Management System is to support all departments of the organisation to be compliant to the Security Requirements, Annexes, and other national and international regulations and advice and support top management and all security risk related employees of the Organisation.

To establish a successful Security Risk Management System it should contain the following: Organisation Values and the Security Policy, a Mission and Vision for security risks matters, security risks requirements which should be mandated, guideline and practices.

For tactical matter the Security Year plan and Security Multi Year plan with recommended strategic goals and in addition the Security Risk Year Report.

Organisations are advised to implement a risk-based security management system for people, property, products, processes, information, and information systems throughout the Organisation industry value chain. A Security Risk Management Programme is necessary to manage Business Impact, Threat & Vulnerabilities which result in a risk profile.

Fig. 1
Example of the Security Risk Management System

4 Security Risk Assessment

A Security Requirement example is to conduct a Security Risk Assessment. Organisations need to establish and maintain procedures for the ongoing identification and assessment of security threats and security management-related threats and risks, and the identification and implementation of necessary management control measures.

Security threats and risk identification, assessment and control methods should, as a minimum, be appropriate to the nature and scale of the operations. This assessment shall consider the likelihood of an event and all of its consequences, e.g. impact.

Assessment of Security risks is a continuous process and the cornerstone of all routine protection measures and non-routine contingency plans.

Skills, systems and contacts should be in place to ensure that risk information is collected, collated, evaluated and (controlled) disseminated.

Security Risk Assessment is the most essential component of the Security Risk Management process. A thorough evaluation of threat, vulnerability/exposure and potential impact is the foundation for all Security arrangements. It makes Security authoritative and cost-effective. It also is an important tool for major business decisions e.g. investments, new projects and divestments.

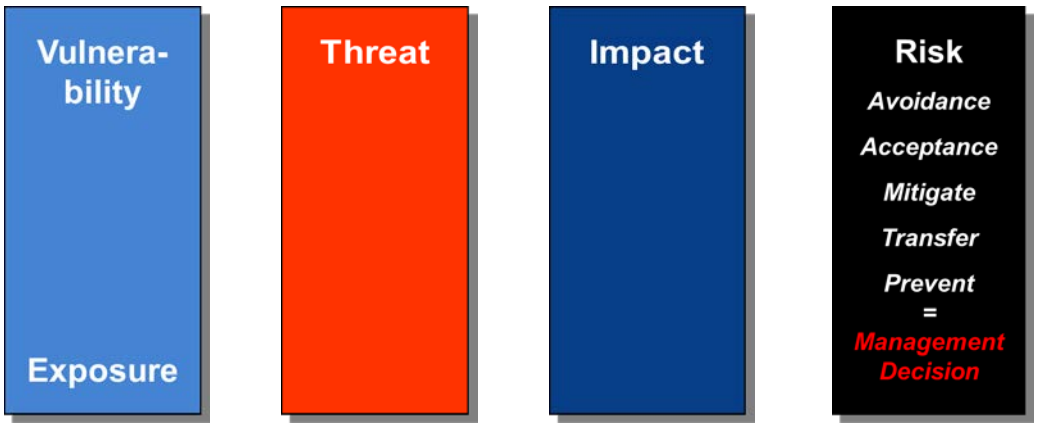

Fig. 2
RISK overview

5 Application of Risk Analysis

Risk analysis, informing the public, and implementing preventive measures, are all appropriate actions to promote sustainable development, which forms a natural part of protecting and improving environment, health and lives of population. Such activities also suitably improve security and economic interests, and help provide accurate information to the population. Also in accordance with the principle of good administration of municipal affairs they certainly encourage social dialogue and public participation in decision-making process to the extent where the public is assured with clear, harmonized and general awareness of the different levels of risks to which it is exposed. It is clear that it will take time to establish such an approach, but the first step is to define the issue more precisely. Risk analysis is thus of both natures: the starting point, and the mean of helping to achieve the goal in the prevention and preparedness effectively.

It can be anticipated with a high level probability that a strategy will be created, that will within the European Union countries focus on enhancement of prevention and improvement of management and interventions in the field of natural and technological risks.

Knowing where the source of risk is, and what it represents is a criterion for the development of effective prevention measures. By their nature, the risks are of an abstract character and their recurrence is unlikely, until they occur. Risk analysis and development of tools (risk analysis methods) is the first challenge we must initiate in this context. To achieve effectiveness this instrument must meet certain requirements: firstly it must allow comparisons among various areas, and it must be accessible and helpful in providing a basis for decision-making process at all levels.

Risk analysis can serve as a base for many applications, such as public notification, preparation of emergency plans, summarization of risks in urban planning, and implementation of additional preventive measures where necessary.

There are strong arguments in favor of a risk analysis harmonization. An ideal situation would be to achieve a harmonized methodology in evey country, as well as throughout the EU.

To achieve this, the population must possess at least minimum information about various risks that exist in the area where they live, or plan to live even just for a limited period of time. This information must be accompanied by recommendations of measures to be taken in

the event of an accident or disaster. Risk analysis according to the general criteria will allow achieving a consistent level of public awareness. It will also provide for more rational use of resources dedicated to prevention by supporting their predisposition based on general criteria when urgent remedial action is needed by improving allocation of resources at all levels. If it is known which areas are threatened, it would help to avoid financing certain projects in those areas, if it can be assumed that investments could be lost there in such events as natural disasters.

The actual use and importance of implementing risk analysis is particularly reflected in the following areas:

Decision-making process

Risk analysis results are mainly applicable within the decision making process of regulating risks when assessing adequacy, efficiency, and effectiveness of resources used for dealing with emergencies and crisis situations. Risk analysis is a basic, essential, and pre-evaluated indicator of appropriate decisions in the field of crisis management, development of strategies, plans and proposals.

Public information

An important objective of risk analysis is to give information to the population that might suffer from the consequences of a natural or industrial disaster. It is evident that the population must not only be aware of existence of such risks, but must also receive adequate information about an appropriate behavior in the event of an accident or disaster. Besides the local residents who ought to be informed, there are many other entities interested in that kind of information for a variety of reasons. Those are mainly industrial and commercial businesses, farmers, and those traders, for whom the common interests of local residents is the matter of their economic survival. Elected representatives must also use this information as the basis for a series of decisions and approaches, especially in the context of urban planning and land use. Reliable information also needs to be available to operators and managers of technical systems - water, gas, electric and telecommunications organizations, etc. especially before purchasing the land. Such operators must also use that type of information to make decisions about the operation and location of the standby devices. Some professions, such as lawyers and insurers, also have a clear interest in information about the level of risk at a given location.

Crisis and emergency plans

Besides the need to inform the public, risk analysis should also be used for the preparation of crisis and emergency plans in order to anticipate the optimal management of emergency and crises situations, and organize rescue units. An emergency plan should mainly determine the direction of use in case of disaster, identify places for emergency accommodation and if necessary also evacuation routes. In this context the way to ensure continuation of essential services (energy, telecommunications, water distribution etc.) must also be contemplated.

Spatial planning

If there is a source of risk identified in an assigned area, it then may be considered for the purposes of a territorial development. Certain decisions e.g. on urban planning, should be assumed at the local level. However, decision making process must take such risks into account. Presumably affected persons must be fully involved in the process, and duly informed of the presence of risks as well as the level of risks. Specifying the area affected by various risks should also enable managers of relevant bodies to take steps to reduce a level of the risk, or to mitigate the consequences if the level of the risk is too high, i.e. where the affected area is too vulnerable.

Nevertheless it should be noted that in compliance with the principle of subsidiarity current measures such as preparation of emergency and contingency plans, consideration of risk areas in urban planning, etc., must be adopted at the local level.

Key factors to success

Organisations must have Senior Management Commitment stated by the Security Policy of the organisation and in addition staff involvement, line management responsibility, and functional leadership. Furthermore a concise, clear security management system, adequate resources, and costs management. For the future success the organisation must have a vision and transparency for security and have excellent communication lines. It is also crucial to initiate Security Awareness Trainings and Competence Trainings for security responsible(s).

Hereafter you see the ingredient to create a security risk overview e.g. a Security Risk Matrix.

Typical examples of vulnerability

- Location and neighbouring sites
- High consequence hazardous product
- High-quality product
- High-value information
- Animal testing
- High-profile Company
- High-profile Management
- Expatriates
- Off-site product distribution and subsequent reliance on 3rd party security coverage
- Use of certain Contract Companies
- Controversial Third Parties on-site
- Poor physical security arrangements
- Low level of security awareness

Typical examples of threats

- Intrusion
  Secure area; restricted/vital area
- Petty Crime
  Minor vandalism; minor theft (internal and external); pick pocketing; nuisance
- Malicious Activity
  Major vandalism; bomb threat; strike; labour unrest; demonstration; blockade; site occupation
- Workplace Violence
  Stalking; abusive behaviour; (sexual) harassment; intimidation; bullying; racism; discrimination; verbal violence; physical violence
- Serious Crime
  Arson; major theft (internal and external); carjacking; burglary; extortion; blackmail; sabotage; product contamination
- Fraudulent Acting
  Forgery; bribery; swindle; deceit; fraud
- Information related Crime
  Business espionage (private party and government); illegal information brokering; leaking information; theft of information; data manipulation
- Violent Crime
  Rape; robbery (single person); assault; murder; bombing; mail bombing; kidnapping; hostage taking

- Organized Crime
  Robbery (gang); infiltration; product counterfeiting and adulteration; money laundering; illegal trading
- Militant Activism
  Violent acts by militant activists
- Civil Disorder
  Political unrest; social unrest
- Armed Conflict
  Guerrilla; civil war; low intensity war; regional war
- Terrorism
  National terrorism; international terrorism
- Public Security
  Poorly resourced; ill-trained; corrupt; unreliable; inefficient; involved in criminal acts

Potential Impact

- People – staff, clients, visitors, contractors, communities
- Business activities
- Assets
- Environment
- Financial position
- Reputation – locally, nationally and internationally

Risk Matrix

The output of the vulnerability, threats and potential impact will result in the Security Risk for the organisation. To make it visible it is showed in a Security Risk Matrix.

The risk rating and risk band is dependent on the likelihood and severity ratings you assign to it. To assign these with any level of accuracy, you need to understand the nature of the risk that you face. [4]

	SEVERITY				
LIKELIHOOD	5	4	3	2	1
5	High	High	High	Medium	Medium
4	High	High	Medium	Medium	Low
3	High	Medium	Medium	Low	Low
2	Medium	Medium	Low	Low	Low
1	Medium	Low	Low	Low	Low

Fig. 3
Risk Rating = Likelihood x Severity

6 Summary

Threat and Vulnerability/Risk Assessments is not new, but increasing focuses on formalised and auditable process. A number of methodologies exist and are in use. Many of those methodologies have a common approach. It is not yet a matter of regulation; however it is now accepted as Best Practice and good business sense.

Absence of a formal Security Risk Management System which includes a formal Risk Assessment may be viewed as indicative of a lack of due diligence and effective risk management.

Due diligence in a nutshell is the process of separating facts from fiction for the purpose of legal compliance and evaluation of security risks.

Operational Requirements are a must if security objectives are to be achieved in the most efficient and effective manner.

The Operational Requirement is a statement of needs based on a thorough and systematic assessment of the problems to be addressed and the desired outcomes and an essential part of the Security Risk Management System.

Are you looking for solutions in your organisation to reduce security incidents and mitigate risks? Use the corporate security risk approach.

An understatement is that Security Risk Awareness is the single, most important part of an organisation policy together with requirements, guideline, and security risk assessment.

Literature

[1] *Threat level from international terrorism raised: PM press statement* [online]. [cit. 2014-10-25]. Available at: https://www.gov.uk/government/speeches/threat-level-from-international-terrorism-raised-pm-press-conference

[2] *What Is Security Intelligence and Why Does It Matter Today?* [online]. [cit. 2014-10-25]. Available at: http://wptemp.erdiscovery.com/what-is-security-intelligence-and-why-does-it-matter-today/

[3] *ISO 28002 – Supply Chain Security and Resilience.*

[4] *Risk Management with Gordon Wyllie* [online]. [cit. 2014-10-25]. Available at: http://www.mindgenius.de/Resources/Articles/Process-Improvement/Risk-Management-2.html

Informace o autorovi

Mike Zeegers

Od roku 1998 zastává pozici manažera bezpečnostních rizik u mezinárodních organizací (Logica-CMG – mezinárodní organizace informačních a komunikačních technologií, DSM – chemická nadnárodní společnost, Akademické lékařské centrum v Amsterodamu). Ředitel pro Evropu u Corporate&Executive Solution v Kentu (Velká Británie). Pracoval 14 let u policie, 11 let byl výkonným ředitelem organizace zabývající se bezpečnostním zařízením a integrovanými bezpečnostními systémy.

V odborné praxi se zaměřuje hlavně na kritickou infrastrukturu v Evropě, energetický sektor, oblast chemie a ropy, dopravu, telekomunikace a bankovní sektor. Získal magisterský titul v managementu bezpečnostních rizik.

Autor mnoha studií z oblasti bezpečnostního managementu a informační bezpečnosti. V minulých letech byl členem řešitelských týmů a vedoucím několika projektů financovaných

Evropskou komisí. Je předseda evropské Energy Infrastructure Security Network (EISN) a člen rady Overseas Security Advisory Council (OSAC) vedeným velvyslanectvím USA v Haagu. Kromě mnoha dalších pozic je také poradce Evropské komise v oblasti bezpečnostních rizik.