CRO briefing
Emerging Risks Initiative – Position Paper

Critical Information Infrastructure

November 2008

Critical Information Infrastructure
The digital economy's Achilles heel

Executive Summary

The purpose of this paper is to raise awareness of the issues created by critical information infrastructure. It is intended primarily for an insurance, reinsurance and risk management audience and sets out to delineate current knowledge, as a primer for individual practitioner's own research and development. Where possible, the authors have identified opportunities for the advancement of expertise. These include opportunities to link with Government sponsored initiatives, as well as opportunities to pioneer the development of new capabilities and solutions.

Information infrastructure is critical to the economic, social and political functioning of any industrialised economy. Loss or damage to this infrastructure can result in loss of life, as well as economic, social and political consequences.

Computer hardware, software and data can be compromised by viruses, hacker attacks, malfunction, human error in running a system or by service interruption of telecom operations and internet services. Such events can include physical damage and may have tangible economic effects. For example, they can result in loss of profits and increased cost of working, arising from a need to copy lost or corrupted data from backups or in a worst case scenario, recreating data from files. Risk to reputation for good security of service and the associated business risk is a further complication.

A loss event such as a fire or an explosion, that damages or destroys a computer or components of a network, is something that insurers can assess and price. Underwriters have a significant bank of risk management knowledge, loss statistics, and pricing expertise to call upon when evaluating risks of this kind. It is therefore commonplace for a property policy to cover loss of hardware and storage media, although indemnity for data and software losses is normally limited to the cost of restoring files from backup data. Loss events causing non-physical damage or third party losses are however, problematic.

Liability issues in the context of information infrastructure are extremely complex, particularly in view of the global reach of networks. The limited availability and incomplete nature of loss statistics, coupled with asymmetric understanding of the risk as between the operator and insurer, means that the insurance industry has a restricted ability to respond to these events.

It became clear during the writing of this paper, that a high level of collaboration between industry, information technology providers and the mathematical sciences will be necessary in order to find better ways of dealing with the risks presented by critical information infrastructure.

In summary, this paper sets out to introduce the challenges presented by these risks, before going on to consider issues of risk quantification and risk management. The paper concludes with a review of the logical steps that could be taken by individual insurance and reinsurance companies in order to better manage the issues raised.

01
Critical Information Infrastructure: A complex challenge

In industrialised societies, computers are interconnected to form a complex communication mesh, characterised by common hubs servicing dispersed users. This interconnectivity is called “network infrastructure”.

The rapid transmission and processing of data, using network infrastructure, is critical to the well being of both producers and consumers. Network failure has the potential for serious economic and social impacts.

Network Infrastructure

Network infrastructure exists on three levels that are set out in the table below. Services build upon each other and unavailability in the lower levels will cause disruption in the higher ones, if there is no backup.

The substance of networked infrastructure is interconnected, dispersed, technically complex, and potentially, easily accessible. All these characteristics create potential for failures that can impact the service directly or increase the vulnerability of the network to malicious damage. Scenarios include accidental physical damage to network components; equipment malfunction or failure; and the consequences of deliberate damage at the physical, transmission or service levels. Each layer of a networked infrastructure has different vulnerabilities.

Pervasive nature of networks

The pervasiveness of networked infrastructure means that virtually all business sectors are subject to critical information infrastructure risk.

Infrastructure	Description	Examples
Service	Higher level infrastructures using the lower transmission layers	WWW Email Virtual Private Networks Video on Demand Voice over the Internet P
Summary of Issues affecting service function The interconnectivity and dispersal of networks creates an opportunity for malicious damage in what is often referred to as a “cyber attack”. This threat is most relevant at the service level, although some forms of cyber attack have the potential to work back through the network hierarchy and have a additional impact on the transmission layer which may even be used for the attack.		
Transmission	Transportation of information through transport protocols	Telephony Radio/TV Broadcast Internet (IP) transport
Summary of issues affecting transmission function Malfunction of transmission equipment also has the potential to interrupt service, potential exposures including configuration errors and “bugs” in hardware or software.		
Physical	Means to transmit electronic signals, either by wire or radio including devices that relay or receive	Fibre Optic Lines Copper Networks Radio Transmitters
Summary of issues affecting physical function Natural disasters have an obvious potential to disrupt services through damage or destruction of physical and transmission equipment. Exposure to natural hazards such as earthquake, storm, flood, bush fire and volcano are in varying degrees relevant, depending upon the location of equipment. Even solar disturbances and cosmic electromagnetic fields can have effects in the case of radio based transmission.		

Table 1 ***Infrastructure and key issues***

Although not limited to these, key industries exposed include:

- Finance
- Health Care
- Energy & Utilities
- Communications
- Food Safety
- Government
- Water
- Transportation

The pervasive nature of software

In the same way that computer networks are found almost everywhere, software is also pervasive. This creates risks of systemic vulnerability and systemic failure.

Case Study 1
Pervasive Software

Y2K

At the turn of millennium, it was feared that computer systems around the world would fail to detect the date change between the years 1900 and 2000. Experts predicted that this programming glitch would lead to cascading and disastrous consequences, ranging from power blackouts, to errors in financial transactions and failures of satellite and telecommunication systems. Some predicted catastrophic consequences for the world economy.

We will never know whether the massive coordinated efforts undertaken by governments and businesses around the world prevented a catastrophic global infrastructure failure but this was an expensive exercise, resulting in over US $ 100 billion in government and direct business costs.

Strong competition, demand for new products and short product cycles, mean that it is almost impossible to produce error free software. This creates hazards for the end user who may find their software does not work as intended (or does not work at all) and a risk for the software seller who may have a liability in contract or at tort.

Mass Market Software

Home computers running mass market software are not traditionally regarded as forming part of critical information infrastructure but they do present a risk of being hijacked for Denial of Service purposes, spreading viruses, worms etc. Again, the pervasive nature of the software used, creates risks of systemic vulnerability and systemic failure.

Limitations of current laws

Current laws do not always reflect the way that rights and responsibilities have shifted. In many countries, laws relating to the sale of goods are based on the practices of the traditional economy. When these laws were framed, critical information infrastructure was unimaginable and in most jurisdictions, application of sale of goods principles would attach an unacceptable level of risk to the seller.

Managing Liabilities

At present, both hardware and software producers use the law to restrict potential liabilities to end users.

Software liabilities

In the software market, licence agreements are used as a mechanism by which the seller can manage down their risk to a level that is acceptable to them.

Hardware liabilities

The way that hardware liabilities are managed varies from country to country. In some territories hardware sellers place a contractual limitation on liability or may disclaim liability altogether. Elsewhere, this is not permitted as a matter of national law, for example under laws implementing the EU Products Liability Directive.

Insuring Software & Hardware Failure

Insurer's liabilities potentially arise through the operation of negligence and contract laws but in practice, there have been few cases of claims being brought against hardware manufacturers or software authors relating to critical information infrastructure.

Property damage or personal injury arising from a failure can be insured and financial loss protection may also be available, depending upon the risk appetite of the insurer concerned.

02
Quantifying the Risk

Losses in the context of computers and networks can have different causes. Whether insurance cover is available and the scope of such cover will depend on the cause of the loss. While the consequences of physical damage are usually covered, insurance cover for non-physical losses can be difficult to obtain and may be restricted. Operators also need to be aware of the potential for indirect losses, such as investment portfolio impacts, that are generally considered to be uninsurable.

Physical Damage

A fire or an explosion, damaging or destroying one or more components of a networked infrastructure, is a typical example for a loss event that could impact the physical layer.

Case Study 2
Accidental Damage

2008 - Damage to undersea fibre-optics communication cable off the coast of Egypt

Although the exact cause cannot be confirmed at this time, it is believed that a dragging ship's anchor damaged several undersea fibre optic telecommunication cables off the coast of Egypt. This damage to cables resulted in the loss of internet and communication links to several countries in the Middle East region and Indian subcontinent.

Internet traffic was rerouted and restored within a few days but these events demonstrate the vulnerability of telecommunication infrastructure to accidental damage.

Property risks of this kind are normally quantifiable, using traditional underwriting methodologies and a property policy would normally cover the loss of hardware and storage media as the result of an insured event. This however, is only a partial insurance solution as indemnity for data and software is normally limited to the cost for restoring from backups. No value is assigned to the creation of intellectual content that may be lost, such aspects being essentially unquantifiable by underwriters and therefore very difficult to insure.

Operator Error

Human error has always been a significant underwriting feature and in traditional markets, underwriters are used to evaluating the training and employment practices of machinery operators. The challenge is that, while this is relatively straight forward when assessing a risk involving, for example moving vehicles, the situation is complex when viewing the IT environment. Skills are constantly developing and standards change, making it difficult for underwriters to arrive at a settled understanding.

Case Study 3
Operator Error

2003 - Electric power grid failure in North America

A failure to respond to warning indicators resulted in a failure cascade through the entire power generation and distribution system. This grid failure encompassed the tripping or shutting down of 260 fossil-fuel power plants and 20 nuclear power plants.

Huge areas of the United States of America and Canada were affected. Over 50 million people and hundreds of thousands of businesses were without electricity for almost four days.

The economic cost of this blackout was been variously estimated at between US $6 and US $10 billion.

Custom Software

Custom software forms a substantial part of information infrastructure and represents a very significant underwriting challenge. It is based on the end users specific requirements but usually includes re-use of previously developed code in order to increase the productivity of the custom software author.

The accountabilities of the custom software author will typically be set out within a system development contract. Such a contract will normally incorporate terms and conditions for the implementation of the new system, integration with existing systems, staff training and subsequent system support. Sometimes custom software is developed by the end user's staff in-house and accountability for such work is likely to be highly variable, depending upon individual circumstances. In addition, whether using a software house or in-house staff, problems identified long after system implementation are often difficult to correct. Original authors are often no longer available to do corrective work, having either moved to other projects or companies, in what can be a very fluid labour market.

It is almost impossible for insurers to assess the reliability of custom software.

Interconnectivity - Liability Cascades

Interconnectivity creates a particular challenge for liability insurers. Underwriters have particular difficulty in assessing the domino effects that can pass through a network, creating what are essentially unknown consequences. The networked nature of Critical Information Infrastructure means that mapping causality, connectivity and potential cascade effects would be incredibly complex, time consuming and expensive. Such mapping would also be out of date almost as soon as created and would not resolve issues of apportionment where more than one operator is at fault.

Terrorism – The limits of insurability

One potential cause of loss or damage to Physical Critical Information Infrastructure is terrorism. The insurance market can meet the demand for insurance against most non nuclear, chemical or biological terrorist attacks but very exposed structures may be excluded from cover and Government backed solutions, such as pools, may apply.

Case Study 4
Terrorism

9-11 - Destruction of Verizon's telecommunication vault

Verizon is the largest provider of wired and wireless telecommunication services to New York's financial district.

On 9-11, Verizon's critical switching equipment and cable vaults sustained serious damage. This shut down both wireless and landline telecommunication services to thousands of residential and business customers, affecting critical public safety and rescue operations.

Rapid recovery operations proved once again the importance of emergency preparedness and contingency planning in quickly restoring the telecommunication capabilities to the financial district.

Cyber Risks

At the most mundane level, failure to protect access codes can give a potential cyber attacker an immense opportunity to do harm while posing as an authorised user or system administrator. Prevention is a matter of good risk management.

Motivations for Attack

Networked Infrastructure is vital to the proper functioning of the social, economic, military and political activities of a modern state. Consequently, states and terrorist organisations have a potential rationale to bring down or compromise networks in pursuit of political objectives.

Criminal activity constitutes a further threat. This can take a number of different forms including;

- Malicious damage
- Extortion
- Monetary theft
- Information or intellectual property theft

While monetary and information theft have the potential to undermine public, business and government confidence in networked infrastructure, activities of this kind would not normally result in damage to infrastructure.

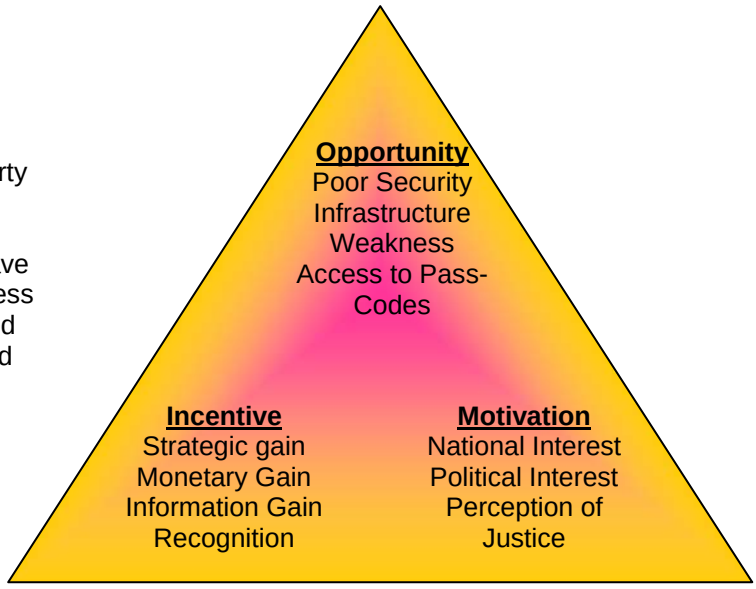


Figure 1 ***Some Motivations for Cyber Attack***

Malicious damage may be motivated by revenge for a perceived slight; curiosity to see what will happen; extortion; or as a way of seeking publicity or recognition.

Multi Layered Attack

The greatest potential for damage arises from an attack that combines a number of different methods. One scenario is a combined assault on both the physical layer and the transmission layer. This demands some sophistication on the part of the attacker because multiple attacking devices / methodologies are necessary. The first step, in an attack of this kind, is to create a bottleneck on the physical layer by reducing the capacity of the network involving, for example, the destruction of fibre optic cables. The second step involves an attempt to overload the network to provoke a collapse. This collapse can be achieved by increasing the traffic on the transmission layer using software designed to take control of a network of computers, that are then used to launch so many messages that the target system crashes.

Otherwise, the methods used will vary with the layer of the network infrastructure attacked. Figure 1 provides a summary of potential motivations.

Underwriting Cyber Attack

Cyber attacks do not usually cause physical damage but definitions of physical damage vary. In some countries, damage by a virus would be regarded as a physical loss but elsewhere this is not the case. In either event, cyber attacks can have tangible economic effects. For example, they result in loss of profits and increased cost of working that include copying data from backups, recreating data from files as well as costs of renting hardware, software or office space. They can also cause an overtime expense arising from the need to clean infected software from viruses or manually enter deleted or corrupted data. Finally, they can damage the reputation of a company resulting in loss of customer or supplier confidence.

As we have seen, coverage for such losses brought about by non-physical causes of loss of data or malfunction of software is rarely offered by insurers. If cover is available, it is usually limited and mainly offered to small and medium enterprises.

Assessing Loss Trends

The magnitude of natural hazards is well understood by the insurance industry and is backed up by many years statistics. Processes are also well established to understand accumulations between individual policies to a particular natural hazard (for example, wind storm) and consequently, natural hazards do not of themselves provide a barrier to underwriting. In contrast to this, there is very little data available relating to non-physical losses.

At present, loss information does not always flow freely. For reasons of customer confidence, public reputation, possible negative impact on stock valuation and in some jurisdictions, anti trust considerations, operators are reluctant to share non-physical loss data. Past attempts at pooling market wide loss statistics on an anonymous basis have failed. This lack of reliable data makes insurance risk evaluation and pricing of the cyber element very difficult.

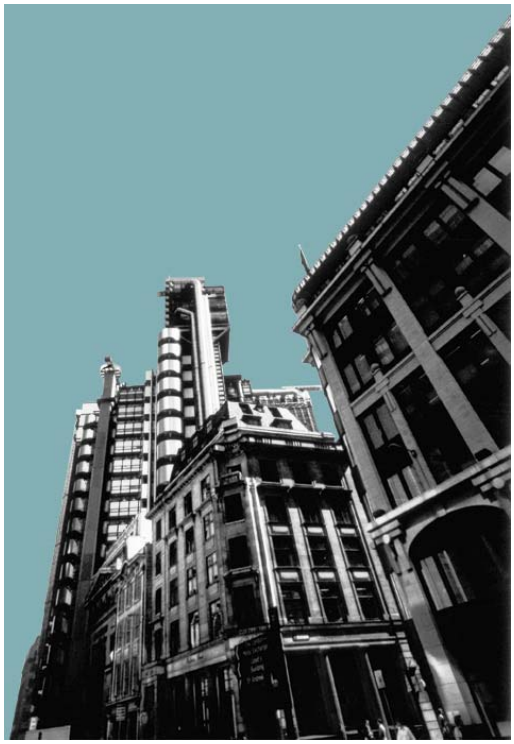
Risks quantification is also difficult. Very little information exists that can used to develop probability or cost models. At best, insurers can develop assumptions and consider best, most likely and worst case scenarios. The usefulness of modelling of this kind will of course depend upon the robustness of the assumptions made. Potential third party liabilities under circumstances where, for example, a firewall proved inadequate are almost impossible to model. Under these circumstances there is no proper basis for informed risk taking by underwriters.

Assessing Technology

The number of products and technologies in use within a typical networked infrastructure has implications for both the frequency and severity of a loss event. Generally, the limited number of technologies used tends to increase the severity of loss scenarios while at the same time, common standards tend to facilitate both effective defence against malicious attack and rapid repair should a loss occur through natural causes, coding, configuration or malicious activity.

Loss History for Cyber Risks

Potential losses arising from cyber attack are among the most difficult to quantify, as society places heavy disincentives on large organisations who fail to protect cyberspace. A good reputation for cyber security is essential for any provider of goods or services and few organisations wish to admit failure. In this environment, the scope for individual insurers or reinsurers to build an extensive data set for losses is limited. Government initiatives are however underway aimed at addressing this issue, and success will assist insurers in future. For example, the European Network and Information Security Agency (ENISA) has a number of tasks including collecting and analysing data on security incidents in Europe.



Emergency Response

A strong partnership between government and business to ensure rapid emergency response is optimal but deregulation, particularly across borders, and lack of information sharing contribute to the difficulty in developing an international approach.

03
Risk Management

Risk Analysis and Incentives

The risk analysis approach of insurance companies assists risk prioritisation and motivates the identification and adoption of best practice by operators. One of the traditional roles of insurance companies has been to provide incentives to invest in risk management through the proper pricing of risk, reflecting by turn good or bad practices. This means that operators with better risk management practices can expect to benefit from lower premiums.

At present, underwriters are unable to price many risks because of the absence of loss data *(see Section 2).* This does not mean that the situation could not be improved by wider adoption of good risk management practices.

Risk Management

Effective risk reduction requires a system-wide approach. Table 2 provides a brief summary of risk management actions relevant to critical information infrastructure however, protecting individual organisations systems, data and networks does not always happen in a perfect way. For example, competitive pressures may prevent organisations from investing enough in avoiding the consequences of failure of their information infrastructure. This is why incentives, such as reduced insurance premiums that reflect good risk practice, can be so important.

Organisations such as the International Organisation for Standardisation (ISO) have a part to play in developing best risk management practices and attention is drawn to ISO 27001 Information Security Management – Specification for Guidance and Use.

Risk Management Actions			
Identify	**Control**	**Protect**	**Maintain**
At risk assets	Information security policy	Systems against malicious software such as viruses and spy ware	Regular back-up of relevant data
Critical dependencies	Information security awareness of employees	IT systems against physical risks	Procedures for testing and implementing changes
	Access to systems and data		Hardware
			Business continuity and disaster recovery plans
			Security patches
			Governance strategy

Table 2 ***Risk Management Actions***

04
A Developing Capability

The Role of Government

Although, many Critical Information Infrastructure assets are owned by global private companies, governments in many countries are responsible for regulatory and oversight aspects, such as in telecom and electric power sectors. Understanding the regulatory environment and the ways in which this interacts with risk, is a key task for underwriters. Adoption of consistent national and global regulations and standards would be welcomed.

In the meantime, governments are helping the insurance industry and it's customers in other ways. In Europe, ENISA's tasks include advising and assisting the Commission and Member States on information security and in their dialogue with industry, to address security-related problems in hardware and software products. ENISA is also actively collecting and analysing data on security incidents in Europe. In the USA, one component of the National Strategy for Homeland Security is the National Strategy to Secure Cyberspace. Initiatives under the National Strategy to Secure Cyberspace encourage the development of a private sector capability to share a complete view of the health of cyberspace.

An Effective Market?

The question remains whether the insurance industry can create an effective market to cover all risks arising from a failure of critical information infrastructure. This may be possible if these risks are both measurable and manageable. The former requires best practices and standards as well as the sharing of information between companies and the insurance sector. The latter is only possible if the failure of information infrastructure does not present loss levels that are too big to be covered by the insurance industry alone.

Developing Know How

A first step for insurers and reinsurers wishing to develop their capability is to identify and acknowledge gaps in current knowledge. As previously noted, these arise primarily from the Business Interruption and third party exposures which have proved particularly difficult to understand and/or quantify.

A number of opportunities exist for insurers and reinsurers to pioneer the development of capabilities and solutions. These opportunities include;

- Developing relationships with industry associations
- Developing a more sophisticated sector analysis, which means understanding each industry sector's use of IT and understanding how service interruption impacts the sector / other parties
- Developing loss frequency assumptions
- Developing loss severity assumptions using techniques such as simulation, emulation, and mathematical modelling
- Developing specialist underwriting skills based on a blend of IT and business knowledge

This work would require a high level of collaboration with industry, information technology providers and the mathematical sciences.

Simulation and emulation modelling will be useful skills. Where these skills do not exist, there may be an opportunity to source expertise through a specialist third party provider.

Establishing Accumulation Models

The development of accumulation models would help the insurance industry to identify, measure and manage exposure.

Figure 2 provides one possible structure for such a model and provides a framework for insurers and reinsurers to better conceptualise exposure.

Accumulation Modelling Template (to repeat across product lines)			
	Physical Layer	**Transmission Layer**	**Service Layer**
Metropolitan Area Network (district up to 50 km^2)			
Wide Area Network (national or across one or more national boundaries)			
Global Area Network			

Figure 2 ***Accumulation Modelling Template***

A template of this kind needs to be supported by suitable assumptions, including assumptions about the mix of activities within Metropolitan Areas, Wide Areas and Global Areas. There is also a need to establish a time off line assumption for the business interruption element. From this, it should be possible to develop portfolio models that take account of the business mix within the portfolio and within the wider society. Accumulation management strategies based on a better understanding of interdependencies, vulnerabilities and controls in critical sectors can then be developed.

Closing Thoughts

The insurance and reinsurance industry still has some way to go in developing a comprehensive solution to the risks presented by Critical Information Infrastructure.

There is a particular need for cooperation and collaboration between the different disciplines that contribute to better understanding. There is also a real need for an inclusive approach to opinion gathering, reflecting the diverse perspectives of stakeholders.

05
The CRO Forum's Emerging Risks Initiative

The Emerging Risks Initiative (ERI) was launched in 2005 to raise awareness of major emerging risks relevant to society and the (re)insurance industry. The initiative is currently chaired by RSA and consists of eight members representing Allianz, AXA, Munich Re, Swiss Re, Zurich Financial Services as well as AIG, Chubb, Insurance Australia Group and RSA.

Emerging risks are by far the biggest challenge for the insurance industry. Emerging risks are risks which may develop or which already exist that are difficult to quantify and may have a large loss potential. Further, emerging risks are marked by a high degree of uncertainty; even basic information, which would help adequately assess the frequency and severity of a given risk, is often lacking. Examples of such risks include climate change, asbestos liabilities, genetic engineering, nanotechnology and terrorism. Insurers have extensive experience in assessing risks but the ever-faster changing risk landscape and its increasingly complex and interconnected risks are making new demands on stakeholders – be they legislators, regulatory authorities, the scientific community, the private sector or civil society – to assume their respective responsibilities in the risk management process.

Governments bear key responsibilities for risk mitigation in society. Jointly with the regulatory authorities, they play a vital role in ensuring the viability of private insurance by creating appropriate legislative and regulatory frameworks. Yet, a systematic approach to risk management has, to date, often been lacking at governmental level, affecting a nation's ability to identify, assess and manage global risks. Professional and systematic risk management would enable governments to prioritise risk mitigation and response measures more adequately. Individual or corporate insureds need to participate in sharing the risk of financial losses. A significant retention of potential loss is a powerful incentive to prevent or mitigate losses and reduces administrative costs by absorbing small, high frequency losses. The insurance industry can create incentives for these mitigation measures by raising awareness of the cost of having undiversified peak exposures. The insurance industry can further add value by contributing risk analysis and management expertise to help insure that entities and regulatory authorities handle their risks optimally.

By absorbing financial and insurance risk, the insurance industry plays an indispensable role in today's economic system. If this is to continue in the future, the industry must minimise surprises. It is therefore crucial to identify and communicate emerging risks to a broader community, thereby fostering a stakeholder dialogue with representatives of a community bound by a shared risk.

This position paper is supported by the CRO forum, which comprises the Chief Risk Officers of the major European and US insurance companies and financial conglomerates. The CRO forum is a professional risk management group focused on developing and promoting industry best practices in risk management. It seeks to present large company views, with three core aims:

- Alignment with regulatory requirements with sophisticated / best practice risk management
- Acknowledgement of group synergies, especially diversification benefits
- Simplification of regulatory interaction

The CRO Forum's views are communicated through it's publications and made available to wider audiences, for example, through the CRO Forum web page at www.croforum.org. The CRO Forum supports the activities of the Emerging Risk Initiative. This Initiative pursues the following goals:

- Raising awareness and promoting stakeholder dialogue
- Developing best practice solutions
- Standardising disclosure and sharing knowledge of key emerging risks

CRO Forum

Tom Grondin
Chief Risk Officer
AEGON

Robert E. Lewis
Senior Vice President, Chief Risk Officer
American International Group, Inc

Thomas C. Wilson
Chief Risk Officer
Allianz

Jim Webber
Chief Risk Officer
Aviva

Jean-Christophe Menioux
Group Chief Risk Officer
AXA

Gerard van Olphen
Chief Financial Officer
Eureko

Olav Jones
CRO Fortis Insurance
CFO Fortis Insurance International
Fortis

Vittorio Chiarvesio
Group Chief Risk Officer
Generali

Rene Cado
Head of Internal Audit & Actuarial Division
Groupama

Eberhard Muller
Group Chief Risk Officer
Hannover Re

Jeroen Potjes
Chief Insurance Risk Officer
ING

Henry Essert
Chief Risk Officer
MetLife

Joachim Oechslin
Group Chief Risk Officer
Munich Re

Marcus Adams
Interim Chief Risk Officer
Prudential

Raj Singh
Group Chief Risk Officer
Swiss Re

Axel Lehmann
Group Chief Risk Officer
Zurich Financial Services

Responsible for content
CRO Forum
Phil Bell, RSA, Chair of the Emerging Risks Initiative

Authors
Scot Gnewuch, AIG
Raphael Marchand, Axa
Nils Diekmann, Munich Re
Andreas Schlayer, Munich Re
Andreas Schraft, Swiss Re
Ashutosh Riswadkar, Zurich

Editor
Keith Baxter, RSA