FERMA™
Federation of European Risk Management Associations

# Network Information Security Platform
# Risk Management Best Practices


**Julien Bedhouche**

**FERMA European Affairs Adviser**

FERMA
Federation of European Risk Management Associations

# Presence

**22 member associations in 20 countries**

**4336 individual members who are responsible for risk management and / or insurance in their organisations**

FERMA
Federation of European Risk Management Associations

# Purpose

Co-ordinate, promote and support the development and use of risk management, insurance and risk financing in Europe

Be a significant stakeholder in the decision making process at the European level on risk management, insurance and risk financing

Focus for 2014 and 2015:

- Profession
- Innovation
- Diversity

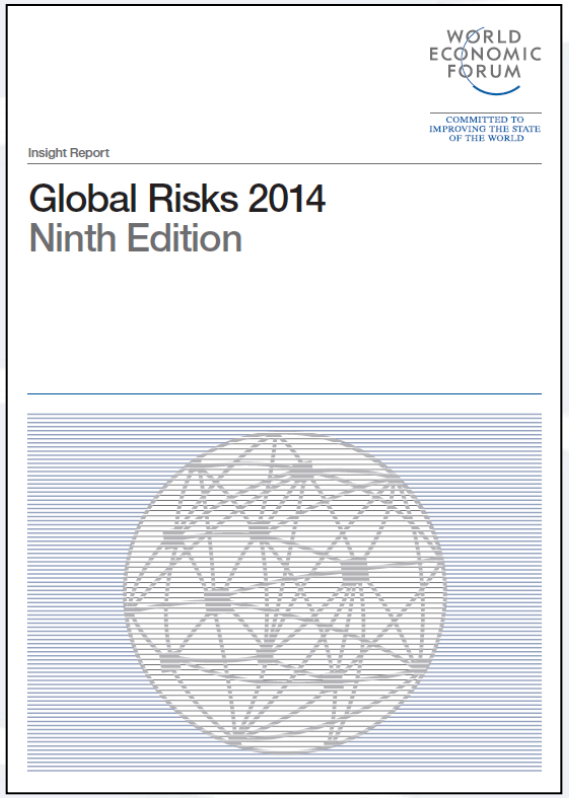
We go where others cannot easily go

Leading risk management and insurance across Europe

FERMA
Federation of European Risk Management Associations

# Cyber is still an emerging risk

- The Global Risks Report from the World Economic Forum 2014 identified Digital Disintegration as one of three key areas of global risk
- While the Internet is designed for resilience, it has little inherent security and so “attackers” have still the advantage over “defenders
- Organizations need to respond through strategic planning, and **review their resilience framework**
- But organizations cannot solve these problems on their own and there is a need for more **joint working at a global, regional and local level**
- There is a **need for more long term thinking**



FERMA
Federation of European Risk Management Associations

# Cybersecurity and Risk Managers

| | |
|---|---|
| Tendency to step away from this subject | **Ceding it to the domain of the CIO - chief information officer or his or her equivalent.** |
| But this is not only an IT risk | **It is an enterprise risk** |
| Risk managers must step up | **Be a stakeholder in its management and a facilitator between boards and operational** |

FERMA
Federation of European Risk Management Associations

# The NISP Guidance Documents

| | |
|---|---|
| "Talk the same language" | • It is a necessity when it comes to risk management, including cyber risk management |
| FERMA believes opportunities for NISP exist to | • Receive, evaluate and promote generic good cyber risk practice<br>• Promote the benefits of cyber risk management frameworks and assurance<br>• Share knowledge, experience and learning by subject and sector |
| But FERMA is cautious about "kite marks" | • They can be manipulated and may inspire over-confidence, especially in fast-changing environment like cybersecurity |

# Kite marks and standards

## This is a challenging area

- Standards require **sharing of intellectual property** about how systems works and yet some are reluctant to share their best knowledge
- Challenges include
  - embracing **the role of risk management**, not only a technical issue
  - defining the **scope of cyber**

## Standards produced to date typically disappointing

- Cyber is complex yet **some government-backed standards are too simple**
- The **definition of a standard takes time and does not match the pace of cyber risks**
- They can encourage a **compliance-led approach**
- **Not fit for SMEs** yet lacking in substance
- **Some good knowledge** and guidance documents are available but are **quickly getting old**
- this is a **global risk** and has to be looked globally

FERMA
Federation of European Risk Management Associations

# Current situations for companies

| | |
|---|---|
| **Most organizations and risk professionals have underestimated** | • the size<br>• the shape<br>• the nature of cyber risk |
| **A skills gap exists between** | • The necessary level of information security: the technology<br>• The current level of information security: the cyber-risk disciplines |
| **Nervousness exists around reporting breaches** | • It hinders cross-sector and country learning about cybersecurity |
| **Risk managers lack confidence in the subject** | • Not just a domain for IT, but weak corporate governance is hindering the ability to deal with technology<br>• Redefining the communication & reporting lines within organisations |

FERMA
Federation of European Risk Management Associations

# The world continues to learn

Cyber is not a traditional risk

- It’s exceeding the pace of information security improvements
- Government activities are inconsistent
- Top Management are not confident with the subject
- Breach monitoring and response solutions require improvement
- **Organizations are seeking benchmarks of what "good" looks like**
- **Insurance can be complex and non-traditional solutions inappropriate. Still early stages.**

FERMA
Federation of European Risk Management Associations

# Cyber insurance

**Global gross written premium**

- **at around $1.5 - $2 billion in 2013**

**Main coverage types:**

- **Liability:** Notice requirements, legal expenses, communications and PR expenses
- **Damages**: forensic studies (replace, restore, recollect digital assets), income losses (business interruption)
- Cyber policies typically have a strict **Bodily Injury and Property Damage Exclusion**

**Coverage typically triggered by**

- **Failure to secure data**
- **Loss caused by an employee**
- **Loss caused by an external person**
- **Loss resulting from theft or disappearance of property such as data on a stolen lap top or missing data storage media**

FERMA
Federation of European Risk Management Associations

# Cyber insurance in the NISP documents (p.3, 4 & 28)

***P.3 Incentives to develop harmonized metrics for calculating insurance risk premiums***

***P.4 Fostering the development of cyber security insurance schemes (tax incentives, public reinsurance to cyber insurance companies, linking the insurance premium to the implementation of risk management best practices***

***P.28 Promoting schemes to cover cyber risk and provide reduced insurance costs if best practice code is adopted***

## For FERMA:

- Coverage needs to be matched to the exposure which varies considerably with the type of business (banking, pharma, energy…)
- The same scheme or metrics will not suit companies with financial data from consumers, design-led businesses, law firms and others with valuable intellectual property, and critical infrastructure
- ***Is it sound to link insurance premiums to certified schemes and not only exposure to risks?***
- ***Could it create a dependency from the administration and/or certification consultants to assess risks and price them?***

FERMA
Federation of European Risk Management Associations

# Shortcoming for Critical National Infrastructures

Insurance markets are reluctant to sell this type of cover

- Any liability that could arise could be impossible for the private sector to indemnify alone

Need for a broader conversation the private and public sector

- Alternatives to develop comprehensive solutions, such as the US Terrorism Risk Insurance Act (TRIA) type of insurance pools, to address CNI cyber exposures

FERMA
Federation of European Risk Management Associations

# Insurers becoming more cyber-savvy

**Independent risk assessments can be useful requirement even if insurance is not purchased**

- It's becoming a more common underwriting requirement

**3rd Party suppliers increasingly asked if they have cyber insurance as a "risk control"**

- It's becoming a condition to do business

**Cyber does not respect physical borders**

- Introduces global insurance program challenges

**Trend for bundled coverage for First and Third party cover**

- Breaking down traditional insurance underwriter and cover silos
- Bundling the insurance cover with appropriate value-added solutions, including support for breach detection and response.

FERMA
Federation of European Risk Management Associations

# CONCLUSIONS 1/2

Cyber insurance provides an umbrella above those covers, not instead of other insurance

To understand what cover is needed, a gap analysis against existing insurance programs is a first step

Some cyber risks will already be covered – and the residual risk evaluated

FERMA
Federation of European Risk Management Associations

# CONCLUSIONS 2/2

A cyber insurance cover may be suitable for the residual risks if cover is available at a worthwhile level and a realistic price

Completing a cyber insurance proposal form for insurance is in itself be a very useful exercise for an organization

Cyber insurance is not a substitute for effective and efficient risk management

FERMA
Federation of European
Risk Management Associations