Cyber Risk – some strategic issues

Paper by **Marie Dequae** - member of the EIOPA Insurance and Reinsurance Stakeholder Group (IRSG)

This paper was drafted as the topic has been identified by the IRSG as one of the strategic areas. All IRSG members have had the opportunity to provide feedback and input.

Based on

- recent articles on this topic
- reactions from users of cyber risk

Content:

Executive summary

European supervisors reported an increased concern about IT related operational risks and cyber attacks as one of the main risks affecting the EU financial system.
Cyber risk is a major threat to businesses in meeting business goals and reputation management and continues to attract considerable attention in media rooms and boardrooms. The cyber risk landscape of tomorrow will look very different to that of today. Emerging risks will come from impact of technology.
Businesses have to understand how cyber risk impacts their operations, how it can be mitigated and then determine their own risk appetite. There is a very broad spectrum of potential losses, depending on the nature of the business and the sector in which it operates. A proactive and more multidisciplinary approach to assessing cyber risk is advised, together with a review of business continuity and crisis management frameworks.
The risks posed by cyber attack present an opportunity for the insurance market. This cyber insurance market is growing rapidly, but challenges come from business' ability to understand their own exposures, the ever-evolving nature of cyber risk and awareness of the different data protection laws globally.
In an environment of changing cyber risk, due to emerging technologies, we see an inadequate global cyber governance framework. A new governance framework is needed that is global and inclusive in nature and based on a multi-stakeholder approach, together with a flexibility to adapt to ever changing threats.
Experience of risk and/or insurance managers with the purchase of cyber insurance cover is shared.
To conclude reference is made to the role of EIOPA to support the insurance sector in this new cyber activity and to get the right oversight information from the national supervisory authorities (NSA's).
EIOPA also has to optimise the management of its own cyber risks.

Introduction

EIOPA's core responsibilities are to support the stability of the financial system and the protection of policyholders. EIOPA is commissioned to monitor and identify trends, potential risks and vulnerabilities stemming from the micro-prudential level, across borders and across sectors.

Preserving financial stability is an important element of Solvency II. One of the specific objectives for Solvency II is improving the risk management of EU insurers and reinsurers (see key macro-prudential risks). One of the 5 strategic goals of EIOPA aimed at improving the functioning of the internal market is to identify, assess, mitigate and manage risks and threats to the financial stability of the insurance sector.

The joint committee of the European Supervisory authorities (ESMA, EBA and EIOPA) reported an increased concern about IT related operational risks and cyber attacks as one of the main risks affecting the EU financial system[1].

Both market participants and competent authorities have increased efforts to address these, but in some cases further understanding and recognition by supervisors and institutions may be necessary.

The European Commission proposes a cyber security strategy for the European Union and outlines the EU's vision and the actions required, based on strongly protecting and promoting citizens' rights, to make the EU's online environment the safest in the world.[2]

We see a focus of insurers to grow in non-life business, which creates an increased competition in this part of the insurance sector.

---

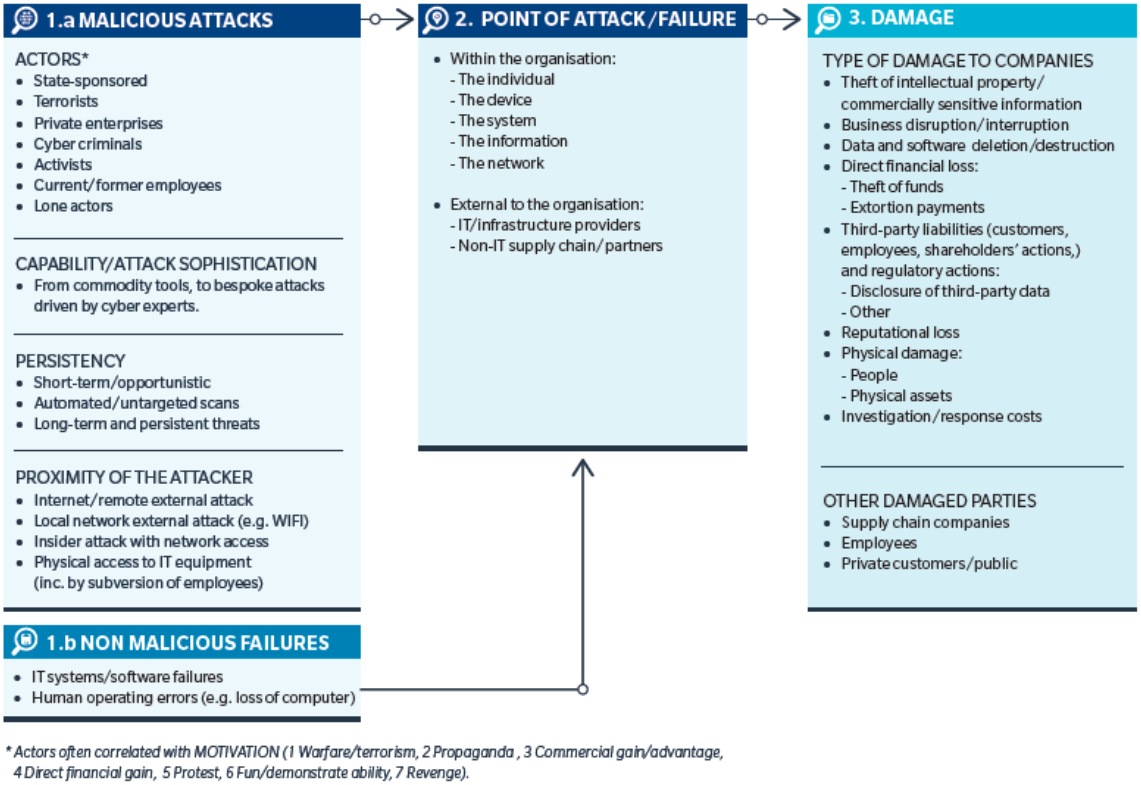
[1] See ESMA, EBA and EIOPA: Joint Committee Report on Risks and Vulnerabilities in the EU financial system, March 2014

[2] **European Commission:** Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions **–** Cybersecurity Strategy of the European Union: an open safe and secure Cyberspace, 7.2.2013 20 pp

1. Risk evolution in the market

In its broadest form, cyber risk is synonymous with IT risk – that is, "the business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise" (ISACA IT Risk Framework).[3]

FIGURE 1: TAXONOMY OF CYBER RISK FOR CORPORATIONS



Source: HM Government and Marsh: UK cyber security

Cyber risk is now a major threat to businesses. Companies increasingly face new exposures, including first- and third-party damage, business interruption and regulatory consequences. The operating environment for many industries is changing dramatically, and becomes more digitally-connected.[4]

The risk of large-scale cyber attacks continues to be considered above average on both dimensions of impact and likelihood. This reflects both the growing sophistication of cyber attacks and the rise of interconnectivity, with a growing number of physical objects connected to the internet ('the internet of things'- IoT) and more and more sensitive personal data (incl. about health and finances) being stored by companies in the cloud. With the evolution of the cloud technology the impression is that the cloud is no more vulnerable than (often aging) poorly protected 'own' made databases. In the USA alone cyber crime already costs an estimated 100 bn $ each year. The current internet was not developed with such security concerns in mind and as such a big need arises for mechanisms to maintain a unified and resilient network or an active Internet Governance.[5] (see §5)
First, as more business activities move online and as more consumers around the world connect to the Internet, and as autonomous devices are connected ("the Internet of things"), the opportunities for cybercrime will grow. Cybercrime remains a growth industry.

[3] See HM Government and Marsh on UK Cyber Security
[4] See Allianz Cyber Risk Guide
[5] World Economic Forum, Global Risks 2015

Second, losses stemming from the theft of IP will also increase as acquiring countries improve their ability to make use of it to produce competing goods.
Considerable attention continues to be given to cyber risk – both in media rooms and boardrooms – across Europe, following a recent string of high-profile attacks on organizations. Perhaps in light of this, respondents to the International Business Resilience Survey 2015 believe that cyber and IT-related events are those most likely to affect their organizations and have the greatest impact on organizational resilience. Respondents appear to be 'comfortable' with the more traditional risks, such as business interruption (BI) and political risk, for example, which received the lowest percentage of responses both in terms of likelihood and impact.[6]

The resilience of IT systems is considered to be the most important factor in meeting business goals and reputation management. This is perhaps unsurprising in the modern age where the computers, email and the internet are all so integral to organizations operating across virtually all industry sectors, and is backed up by the importance placed on the analysis and implementation of control procedures for the resilience of IT systems
It is interesting to note that CEOs place less importance on the resilience of IT systems in relation to reputation management, while giving greater attention to crisis management planning[7].

Given the limited level of cyber risk assessment and cyber incident disclosure, it is not surprising that cyber risks often remain misunderstood or not quantified. We would **recommend** companies take a **proactive approach** to assessing their cyber risk exposures, both in terms of their own activities and their responsibilities to customers and other third parties, and consider more closely the significance and business disruption impact of intangible asset incidents. Further, as cyber cuts across many areas of an organisation, cross functional engagement is key, including risk/compliance, IT, finance and legal.

The *top trends*[8] in the cyber landscape are:

- increasing interconnectivity and "commercialization" of cyber-crime driving greater frequency and severity of incidents, including data breaches;
- data protection legislation will toughen globally. More notifications and significant fines for data breaches in future can be expected;
- business interruption (BI), intellectual property theft and cyber-extortion risk potential increasing. BI costs could be equal to – or exceed – breach losses;
- vulnerability of industrial control systems poses significant threat;
- no silver bullet solution for cyber security.

Potential *risk scenarios*[9] from cyber-attacks/incidents are:

- critical data is lost,
- customers may be lost and business interrupted,
- property damage,
- theft,
- adverse media coverage/damage to reputation/lower market share – 71% of customers said they would leave an organization after a data breach[10],
- regulatory actions and associated fines and penalties,
- profits impacted/value of shares may fall,
- loss of trade secrets/confidential information,
- extortion,

[6] See MARSH report 2015 p.4
[7] See MARSH report 2015 p.8
[8] AGCS, A guide to Cyber Risk
[9] AGCS, a guide to Cyber Risk
[10] Edelman Privacy Risk Index

- breach of contract,
- product recall,
- notification costs and other response costs, i.e. forensic IT,
- network security liability,
- Directors' and Officers' liability.

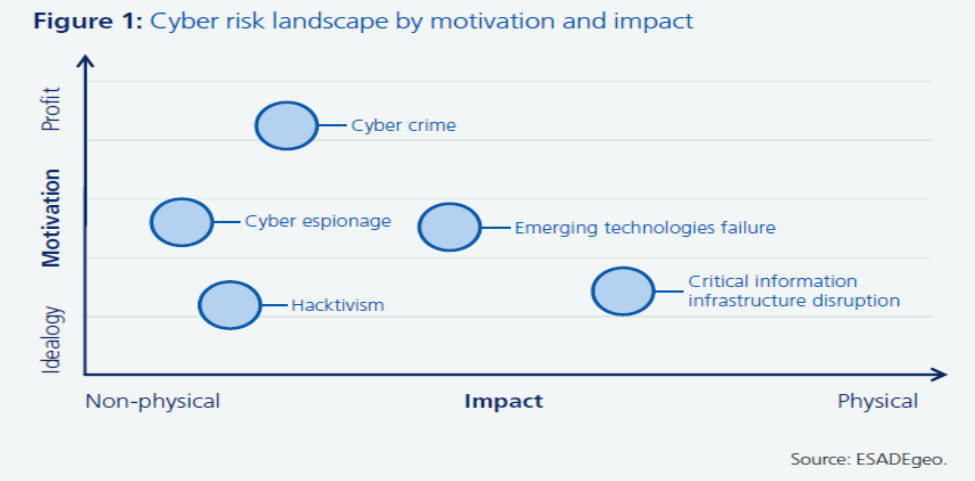
The industry needs to understand cyber risk independently of the insurer to create the right protection mechanisms, cyber models and rating bands.

Cyber risk 2025 – the next 10 years [11]:

- Cyber insurance market could be worth $20bn+ by 2025;
- Liability and data protection risks dominate market today but demand for, and take-up of, business interruption cover will grow over next decade;
- Businesses will be increasingly exposed to – and focused on – supply chain cyber risk;
- Financial institutions, energy, utility, transport and telecommunications sectors to lead widening demand for cover;
- A catastrophic cyber loss is increasingly likely. Governments, businesses and insurers will need to collaborate to protect critical infrastructure.

The cyber risk landscape of tomorrow will look very different to that of today. Emerging risks will come from impact of technology. The risks can also be categorised by impact and motivation:

Figure 1: Cyber risk landscape by motivation and impact



Some *interconnected cyber threats*[12] are:

- estimates suggest a trillion devices could be connected by 2020;
- 'the Internet of Things' will exacerbate cyber vulnerability, bringing increasing potential for physical loss and data breaches;
- cyber criminals will exploit increase in interconnectivity between machines in the supply chain, creating new exposures;
- as technology evolves, aging hardware also becomes vulnerable to attack;
- cloud computing can create systemic risk.

Specific highlights from the Ponemon Institute 2015 Cyber Risk Study research [13] include:

- Information technology assets are 38% more exposed than property assets, with 11% of potential loss to intangible assets covered by insurance, compared with 49% for tangible assets.

[11] AGCS, a guide to Cyber Risk
[12] AGCS, a guide to Cyber Risk
[13] See Aon & Ponemon Institute

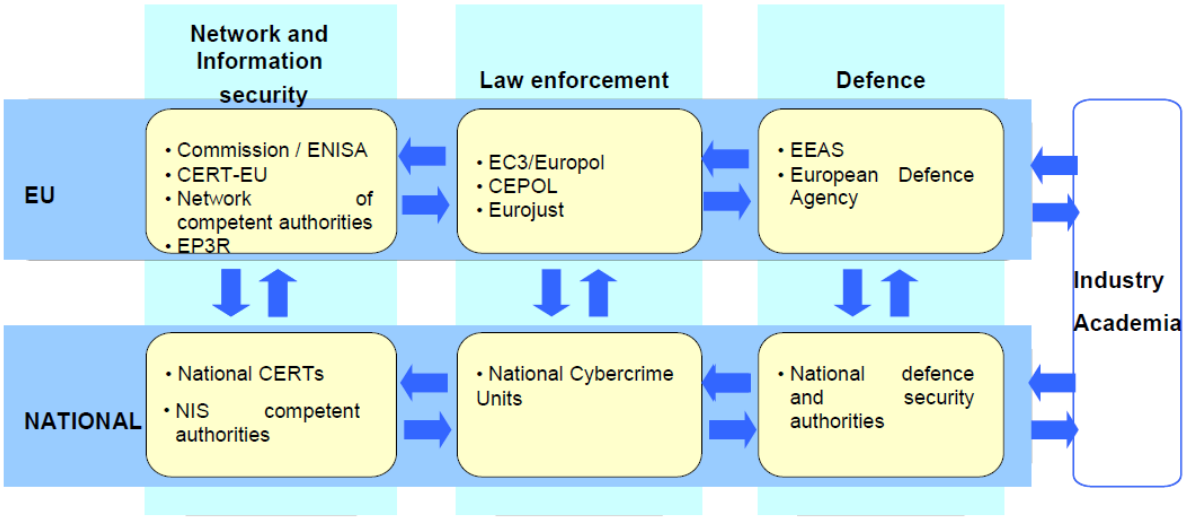
- This is despite the fact that estimated value and maximum loss is on a par for intangible and tangible assets (e.g. probable maximum loss of USD638 million and USD615 million respectively).
- Almost four in ten (38%) of businesses surveyed experienced a material or significantly disruptive loss relating to a security or data breach in the past 24 months. The average financial impact of these incidents was USD1.1 million.
- 37% of businesses would not disclose a material loss to their intangible assets in their financial statements, whereas only 9% would not disclose a material loss to tangible assets.
- Four in ten (44%) determine their businesses' level of cyber risk based on intuition, informal internal assessment, or without any assessment at all.

The likely annual cost (both direct and indirect) to the global economy from cybercrime is estimated at more than $400 billion. A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion. Even the smallest of these figures is more than the national income of most countries and governments and companies underestimate how much risk they face from cybercrime and how quickly this risk can grow[14]. Cybercrime damages trade, competitiveness, innovation and global economic growth. Opportunity cost is the value of forgone activities—opportunities or benefits that cannot be realized because resources have been expended elsewhere. Three kinds of opportunity costs determine the losses from cybercrime: reduced investment in R&D, risk averse behaviour by businesses and consumers that limits Internet use, and increased spending on network defence.

[14] See report from Center for Strategic and International Studies

2. Cyber risk assessment and mitigation

The European Commission asks for all actors to take their responsibility as cyber incidents do not stop at borders in the interconnected digital economy and society. All actors, from NIS competent authorities, CERTs and law enforcement to industry, must take responsibility both nationally and at EU-level and work together to strengthen cyber security.



Source: **European Commission:** Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Cyber security Strategy of the European Union: an open safe and secure Cyberspace, 7.2.2013 20 pp.

Insurance and reinsurance are not alternatives to enterprise risk management (ERM), but should be used to address structural residual risk after risk management steps.
Businesses must understand how cyber risk impacts their operations, how it can be mitigated and then determine their own risk appetite.

Loss categories can be described as in following figure[15]:

[15] **HM Government & Marsh:** UK CYBER SECURITY - the role of insurance in managing and mitigating the risk, March 2015, 32 pp.

FIGURE 3: LOSS CATEGORIES DERIVING FROM CYBER ATTACKS AND NON-MALICIOUS IT FAILURES

	LOSS CATEGORY	DESCRIPTION
A	Intellectual property (IP) theft	Loss of value of an IP asset, expressed in terms of loss of revenue as a result of reduced market share.
B	Business interruption	Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a result of cyber attacks or other non-malicious IT failures.
C	Data and software loss	The cost to reconstitute data or software that has been deleted or corrupted.
D	Cyber extortion	The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
E	Cyber crime/cyber fraud	The direct financial loss suffered by an organisation arising from the use of computers to commit fraud or theft of money, securities, or other property.
F	Breach of privacy event	The cost to investigate and respond to a privacy breach event, including IT forensics and notifying affected data subjects. Third-party liability claims arising from the same incident. Fines from regulators and industry associations.
G	Network failure liabilities	Third-party liabilities arising from certain security events occurring within the organisation's IT network or passing through it in order to attack a third party.
H	Impact on reputation	Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event.
I	Physical asset damage	First-party loss due to the destruction of physical property resulting from cyber attacks.
J	Death and bodily injury	Third-party liability for death and bodily injuries resulting from cyber attacks.
K	Incident investigation and response costs	Direct costs incurred to investigate and "close" the incident and minimise post-incident losses. Applies to all the other categories/events.

Source: Marsh

There is a very broad spectrum of potential losses, depending on the nature of the business and the sector in which it operates. A company is exposed to its own set of cyber risks:

- A financial institution holds a wealth of data on its customers. A theft of which would damage strongly its reputation. Banks also face huge business interruption exposures through the use of electronic trading systems.
- A utility company is more exposed to risks linked to industrial control systems, where a hack could cause catastrophic damage to property or subsequent business interruption.
- A pharmaceutical or tech company will hold valuable intellectual property, while a professional services company will hold sensitive client data.

5 top *cyber risk mitigation tips*[16] are

- Identify key assets at risk and weaknesses such as the "human factor" or over-reliance on third parties
- Create a culture of cyber security and a "think-tank" approach to tackling risk – different stakeholders from the business need to share knowledge
- Implement a crisis response or breach response plan. Test it

[16] AGCS, A guide to Cyber Risk

- Consider how merger and acquisition activity and changes in corporate structures will impact third party data
- Make decisions around which risks to avoid, accept, control or transfer.

Actually we see a limited level of cyber risk assessment and cyber incident disclosure and as such it is unsurprising that cyber risks often remain misunderstood or unquantified. We would recommend companies take a **proactive approach** to assessing their cyber risk exposures and consider more closely the significance and business disruption impact of intangible asset incidents. Further, as cyber cuts across many areas of an organisation, cross functional engagement is key, including risk/compliance, IT, finance and legal. A more **multidisciplinary approach** is advised.

In order to better understand, quantify and protect against cyber risks **more information sharing** is needed. In order to reach an effective cyber resilience assurance a concerted effort among all participants is required to develop and validate a shared, standardized cyber threat quantification framework that incorporates diverse but overlapping approaches to modelling cyber risk[17].

The insurance industry, through CRO Forum is currently establishing infrastructure to better capture statistical cyber risk and loss data. Establishing common cyber reporting standards and practices for coding and **classifying cyber risks** not only will facilitate information sharing, risk identification and assessment, but also form the basis of a properly functioning cyber insurance market.
Businesses can also help by sharing their cyber attack experiences and loss information. A cyber risk database could be modelled on existing loss databases, where anonymity could encourage reporting;[18]A Cyber Catastrophe Stress Test Scenario was developed by the Cambridge Centre for Risk Studies. In this scenario we take an imaginary SITE, which we call the Sybil Corporation, and investigate the impact on the global economy of an insider attack that introduces

[17] WEF & Deloitte: Partnering for Cyber Resilience: Towards the Quantification of cyber threats
[18] ESADEgeo & Zurich Insurance Group

a compromise, or 'Logic Bomb' into their flagship database product used throughout the corporate world. The resulting global macro-economic impact portends an economic downturn driven by a reduced trust in IT by business leaders, investors and consumers, which we call an 'information malaise'. The damage caused by the more extreme variants of Sybil Logic Bomb is almost as severe as the Great Financial Crisis of 2007-2012.[19]
Another recent study by Lloyds and the Cambridge Centre for Risk Studies deals with the scenario of a business blackout and the insurance implications of a cyber attack on the US power grid.[20]

Firms should consider including a comprehensive review of the dependencies of critical IT services and processes in their crisis management plans, and the results of this should be relayed to the C-suite.[21]
Existing **business continuity and crisis management frameworks** should be reviewed to ensure they are properly addressing emerging risks; in particular, data breach scenarios and the resilience of IT systems. The availability of a cyber crisis management plan is of paramount importance to secure organizations' reputations[22].

[19] University of Cambridge, Judge Business School, Center for Risk Studies, Stress Test Scenario - Sybil Logic Bomb Cyber Catastrophe, Systemically Important Technology Enterprises:-Mapping the Consequences of an Interconnected Digital Economy
[20] See Cambridge Centre for Risk Studies and Lloyds: Business Blackout
[21] See MARSH report p. 8
[22] MARSH report**,** International Business Resilience Survey 2015, 11 pp

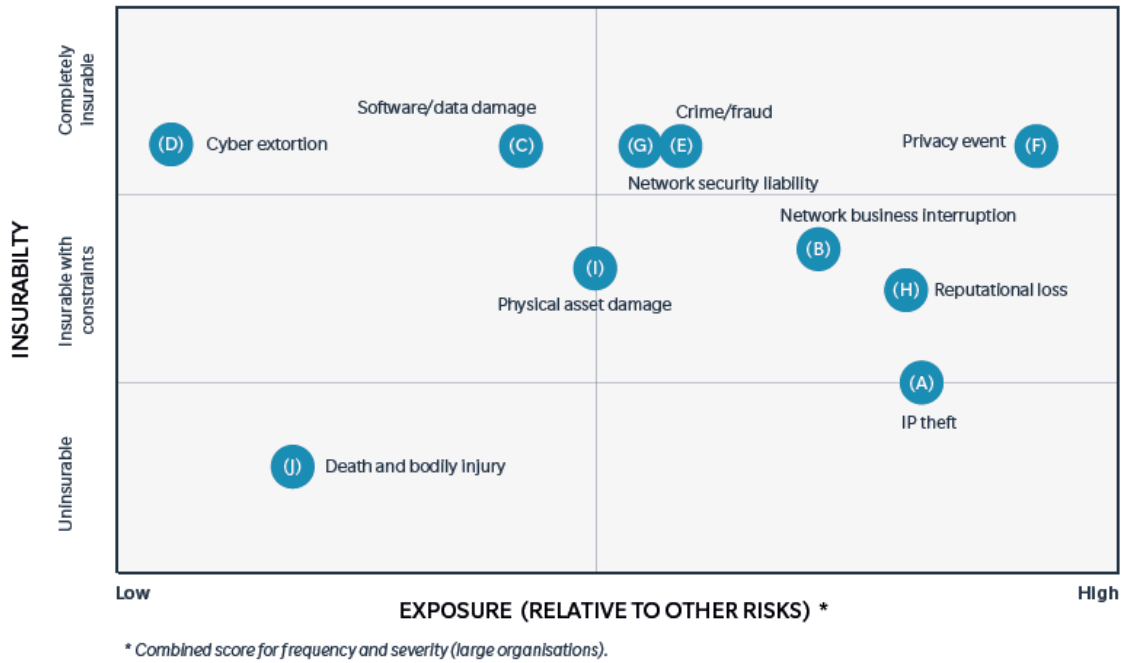
3. The Cyber insurance market and coverage

Currently, the market for the cyber insurance policies is not very developed, and seems to consist of relatively customised policies dominated by a few big insurance providers. Not all cyber protection policies cover litigation and redress costs for instance, partly because it is difficult to establish a correct pricing for such products due to lack of data. However, several insurance companies, including some European companies, are positioning themselves, either with research reports or through product offering in this market, which is expected to grow in the coming years. Some products already on the market cover for instance protection against involuntary breach of privacy regulations and against claims for damages made by third parties if customer data is lost or made public. Even costs of notifying customers, hiring Public Relations consultants, and lack of revenue can be covered in some policies[23].

The cyber insurance market is currently estimated to be worth around **$2bn** in premium worldwide, with US business accounting for approximately 90%.
Fewer than 10% of companies are thought to purchase cyber insurance today. However, the cyber insurance market is expected to grow by double-digit figures year-on-year and could reach **$20bn+** in the next 10 years.

In the next figure the insurability of different risks is compared against the risk exposure deriving from the frequency and severity of each risk.[24]

FIGURE 9: INSURABILITY AND EXPOSURE FOR DIFFERENT CYBER RISKS



[23] EIOPA financial stability report, May 2014

[24] HM Government & Marsh: UK CYBER SECURITY - the role of insurance in managing and mitigating the risk, March 2015, 32 pp.

Top trends in cyber insurance[25] are:

- Exclusions or cover limits in traditional policies will become more commonplace;
- Standalone cyber product to be the main source of liability cover;
- Cyber concept and wordings will be tested, potentially resulting in litigation;
- Cyber insurance market needs volume and diversification;
- More segmentation in future with insurers specializing in certain sectors;
- Lack of education is an obstacle to growth – both in terms of businesses' understanding of exposures and underwriting knowledge;
- In the event of a cyber security incident a speedy response and
- use of third party experts can mitigate losses.

Standalone cyber insurance will continue to evolve as it responds to changes in both cyber risk and regulation. However, such development will bring challenges. There are a number of different policies in the market and many have concepts and wordings that have yet to be tested.
52% of CEOs believe that they have cover, whereas in fact less than 10% do[26].

While the cyber insurance market is growing rapidly, certain factors are holding back even more rapid development:

- businesses' ability to understand their own exposures,
- the ever-evolving nature of cyber risk and
- awareness of the different data protection laws globally

all present challenges.
More companies are using cyber captives to help address the ongoing risk of cyber attack.
The speed of regulatory change in data breach reporting will lead to increased cyber liability cover and even mandatory insurance in some cases.

Cyber risk insurance may provide growth opportunities for insurers once such policies and the understanding of the inherent risks mature. However, these products require thorough risk management, and insurance supervision needs to be adapted to adequately understand the potential risks in such underwriting[27]*.*

In their own governance system insurers have to work on different levels to capture and manage their cyber risk exposures.[28] First a specific risk appetite for cyber risk across all classes of business has to be determined and approved by their Board. Within their formal risk management framework structured processes for understanding cyber risk exposures by class of business have to be activated. In order to consider their gross aggregate exposure to cyber risk, it is important to adopt a scenario-based approach, with several internal scenarios (cfr literature d,e,f).
The national supervisory authorities have to follow up on this and ask for regular reporting.

<u>Education of businesses, brokers, underwriters and insurance supervision is key.</u>

4. *From internal to global cyber governance*

At **company level** it is important for critical infrastructure providers to have an efficient risk governance structure for cyber risk. Following elements are crucial:

- A risk committee, at board level or at executive level,

[25] AGCS, A guide to Cyber Risk
[26] HM government & Marsh/ Uk Cyber Security
[27] EIOPA financial stability report, May 2014
[28] cfr what Lloyd's is requesting from its syndicates

- A chief risk officer and risk function that operate independently of executive management.
- A recovery plan that brings financial, operational, reputational and other critical functions together;
- The use of risk scenarios and stress-testing of financial resilience against these scenarios.

In an environment of changing cyber risk, due to emerging technologies, we see an inadequate **global cyber governance framework**. A new governance framework is needed that is global and inclusive in nature and based on a multi-stakeholder approach, together with a flexibility to adapt tp ever changing threats[29].

The private sector should also take specific steps to mitigate cyber risk and enhance general resilience in the meantime, given the lack of effective global governance. Greater information sharing will play a key role in developing the tools to achieve this, such as a well-functioning insurance market.

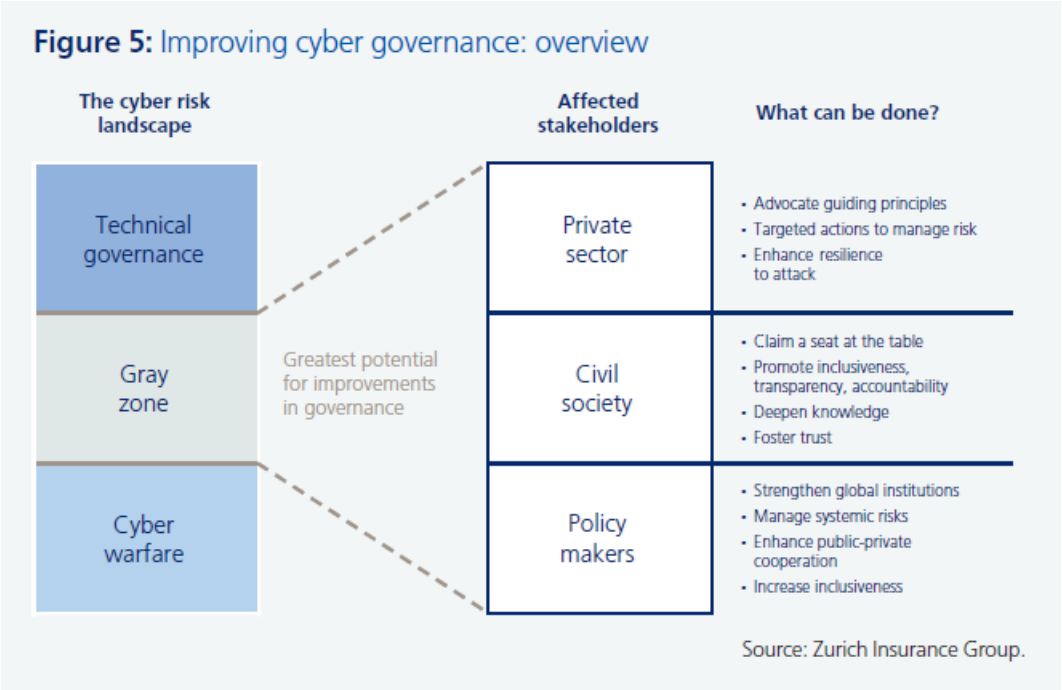
Table 1: Summary of private sector and policymaker recommendations to improve global cyber governance

Recommendation	Proposed mechanism
Business	
Greater information-sharing to mitigate cyber risk.	Insurance industry via the CRO forum. Anonymized business loss reporting via private sector-led initiatives, e.g., FS-ISAC, public-private bodies e.g., ENISA.
Champion common values for global cyber governance in absence of governments' consensus.	Lobby through institutions, particularly privately-led initiatives, e.g., CRO forum and multi-stakeholder dialogue forums, such as WEF.
Take targeted actions to manage cyber risk.	Adopt SANS 20 Critical Security Controls. Further actions needed for larger organizations.
Enhance general resilience to cyber risk.	Built-in redundancy, incident response and business continuity planning, scenario planning and exercises.
Policymaker	
Strengthen those aspects of global governance that have worked properly and isolate them from geopolitical tensions.	Develop informal global cyber networks. Adopt a 'build it and they will come' approach.
Create a system-wide institution for incident response.	G20+20 Cyber Stability Board.
Enhance crisis management to deal with a potential systemic cyber crisis.	Cyber WHO (World Health Organization).
Seek greater public-private cooperation.	Incentivize alignment of public/private interests on cyber security.
Reinforce protection of critical information infrastructures.	Cyber stress tests.

Source: ESADEgeo & Zurich: global cyber governance

[29] ESADEgeo &Zurich, Global Risk Governance, 2015

The current global governance of cyber risks can be viewed as comprising three layers.
First, there is the layer of more technical aspects that help network systems to function properly, by ensuring that all the infrastructure and devices constituting the internet can talk to each other. On this level, global governance is largely effective – following a multi-stakeholder model based on a loose, bottom-up consensus. Today the bulk of financial resources are allocated in this technical layer.
Cyber warfare represents the other end of the spectrum, and includes issues relating to state-sponsored cyber attack, espionage between states, and cyber attacks on critical infrastructure for political purposes. Here a global governance is absent. Between these two extremes is a 'gray zone' – a more diffuse realm where the interests of industry, governments, and individual citizens intersect. Issues addressed in this space include intellectual property rights, cyber attacks by non-state actors on individuals, criminal activity and data protection



Governance, no matter how comprehensive, can never nullify all risks. But effective governance can be the key to keeping risks at manageable level. Given the importance of cyberspace to our world, improving its governance on a global scale is therefore critical.

The national supervisory authorities can follow up on this risk by asking good reporting from Insurers on their oversight framework for cyber risk exposure monitoring (see § 3)

5. *Experience of risk and/or insurance managers with the purchase of cyber insurance cover*[30]

This paragraph is based on informal discussions between 19 European risk and/or insurance managers from automotive, transport, energy, chemicals, food sectors in April 2015.
The purchase of a cyber insurance cover could be understood in the same meaning as in the FERMA Risk and Insurance report 2014, i.e. as **a separate cyber insurance policy, and not as a sum of partial coverage granted under property, liability, and crime policies**.
In the 2014 benchmarking survey, 72% of respondents indicated they do not purchase stand-alone cyber coverage.[31]
In 2016 a renewed benchmarking survey will be organized.

I. <u>There is uncertainty about the purchase decision</u>

- The quoting process relies very much upon the active support of the IT department (qualified by one participant as a "painful and time-consuming exercise").
- The risk exposure exercise, done jointly with IT and legal, may not necessarily reveal the need for **a purchase decision** of a stand-alone insurance coverage for cyber security but rather the necessity of an **additional focus on back up and emergency procedures, but**
- The **market is reliant on third parties** in charge of fairly basic assessments and interviews with the IT department. They are sometimes **not convincing to show they understand the specificities of the business** and its IT risks.
- **There are concerns about the claims payout ratio** of the cyber insurance products.

II. <u>Triggers for a purchase decision are</u>

- **Alignment of views** between IT, legal and the Board about the necessity of a cyber cover.
- **Interim solution** before a Group decision on a global insurance purchase: purchase off the shelf local "cyber" insurance policies for the retail activity in the US only. The limits purchased are low, as is the premium, and the likelihood of collecting any meaningful claim there under.
- A **condition for doing business**: regulators for the banking sector in the US constantly now ask for proof of cyber insurance policy.

III. <u>Best practices are:</u>

- Start conversations with brokers and insurers only after securing the help from IT and Legal (Privacy) departments to **assess exposure and counter measures** with an in-depth analysis;
- A risk map containing risk identification and quantification to be used as reference about the risk exposure;
- Once a year, perform an update with IT people concerning the **values to be covered;**
- A **mapping exercise to compare coverage available** from stand-alone Cyber insurance with what already exist in E&O "traditional" programs. The result may show that some policies already have

[30] Based on information from FERMA
[31] http://www.ferma.eu/about/publications/benchmarking-surveys/benchmarking-survey-2014/

most of the covers (Not buying a stand-alone cyber but have extended the existing program coverages following detailed risk dialogues with the carriers and brokers)

IV. Difficulties and challenges of the quoting process

- It is a complex and decentralized exercise with the IT department, taking a lot of time before reaching useful conclusions.
- IT department has **other priorities** and often feels that insurance is **not an adequate reaction** nor a value proposition for the organization.
- Natural preference for IT for the set up/implementation of adequate and robust Business Continuity and/or Disaster Recovery plans as the most efficient way to manage this type of risk.
- Without the backing of the IT department, the role of the risk/insurance manager could be **limited to due diligence role** about the availability of stand-alone cyber coverage.
- **Cover and available limits changing rapidly**: by the time the organization is ready to start discussing insurance options (i.e. after risk exposure: identification and quantification) the market for such is likely to have evolved substantially.
- **Accumulation of risks**: more and more **sensitive data** of the organization are **hosted externally** (i.e. in the cloud). Great uncertainty about how current insurance solutions can protect from the **failure of multiple hosts** of sensitive data of an organization.

Conclusions

Based on the EC cyber security strategy, and the ever-evolving nature of cyber risk with a focus on increased interconnectivity we see a rapid growing cyber insurance market.
All parties involved should adequately understand all potential risks and opportunities, including for insurers the important underwriting risks. Education, cooperation and information sharing in this area between all stakeholders in this process, businesses (all involved departments), brokers, underwriters and insurance supervision is crucial.
Given the importance of cyberspace to our world, improving its governance on a global scale is critical.

The role for EIOPA is to contribute to ensuring that this risk transfer can occur in a reliable and effective way. As such it is important to support the insurance sector in this new cyber activity and not to suffocate them with modelling and capital requirements that make it impossible for the insurers to close contracts, leaving the industry and commerce with non-fulfilled insurance needs. Instead focusing on knowledge and information gathering from clients (a comprehensive risk assessment) will enable insurers to offer the right coverage at the right time.
EIOPA also can follow up with the NSA's (reporting and visits) how the cyber risk insurance practice is evolving (coverage and claims experience) so that more information is shared and best practice can be spread. EIOPA would usefully issue guidance to NSA's and to industry which would encourage best practice in defining different cyber coverages (e.g. malicious attack/other, first- and third-party losses), in defining quantitative risk appetites and in developing scenarios to test accumulations and so on.

And EIOPA is itself a big data collecting organisation and has to manage its own risks. As such EIOPA has to apply the full risk management process, identifying, assessing, mitigating and managing its risks in order to protect its own financial stability. It is important to build a safe and secure cyber security strategy and where needed look for an adequate insurance cover.

Abbreviations:

CERT	= Computer Emergency Response Team
IoT	= Internet of Things
IT	= information technology
NIS	= network and information security
NSA	= national supervisory authority
SIFI	= Systemically Important Financial Institution
SITE	= Systemically Important Technology Enterprise
WEF	= World Economic Forum
CRO Forum	= Chief Risk Officers' Forum
BI	= Business Interruption

Literature:

a. **Allianz Global Corporate & Specialty,** A Guide to **Cyber Risk,** Managing the Impact of Increasing Interconnectivity, September 2015, 30pp.

b. **AON & Ponemon Institute:** 2015 EMEA Cyber Impact Report – The increasing cyber threat – what is the true cost to business? 2015 12 pp.

c. **Atlantic Council & Zurich Insurance Group:** Risk Nexus: Beyond Data Breaches: global interconnections of cyber risk, April 2014, 28 pp.

d. **Cambridge Centre for Risk Studies:** Cambridge Risk Framework; Cyber catastrophe: Stress Test Scenario: Sybil logic bomb cyber catastrophe scenario, June 2014 45 pp.

e. **Cambridge Centre for Risk Studies:** Cambridge Risk Framework: Technological Catastrophe: Cyber Catastrophe - Profile of a Macro-Catastrophe Threat Type; July 2013 21 pp.

f. **Cambridge Centre for Risk Studies and LLOYDS**: emerging risk report 2015, Society & Security, Business Blackout: The insurance implications of a cyber attack on the US power grid,

g. **Center for Strategic and International Studies,** Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, June 2014, 24 pp.

h. **ESMA, EBA and EIOPA**: Joint Committee Report on Risks and Vulnerabilities in the EU financial system, March 2014, 31 pp.

i. **EIOPA:** Financial Stability Report: The European Insurance Sector - Market for cyber risk insurance policies – May 2014 p.19

j. **ESADEgeo & Zurich Insurance Company Ltd,** Risk Nexus, Global cyber governance: preparing for new business risks, April 2015, 30 pp.

k. **European Commission:** Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions **–** Cybersecurity Strategy of the European Union: an open safe and secure Cyberspace, 7.2.2013 20 pp.

l. **EY**: Mitigating cyber risk for insurers part 1 & 2: insights into cyber security and risk – 2014 20 & 18 pp.

m. **HM Government & Marsh:** UK CYBER SECURITY - the role of insurance in managing and mitigating the risk, March 2015, 32 pp.

n. **MARSH report,** International Business Resilience Survey 2015, 11 pp.

o. **World Economic Forum**, Global Risks 2014 – 9th edition 58 pp.

p. **World Economic Forum**, Global Risks 2015 – 10th edition 64 pp.

q. **World Economic Forum & Deloitte,** Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats, 2014, 17 pp.