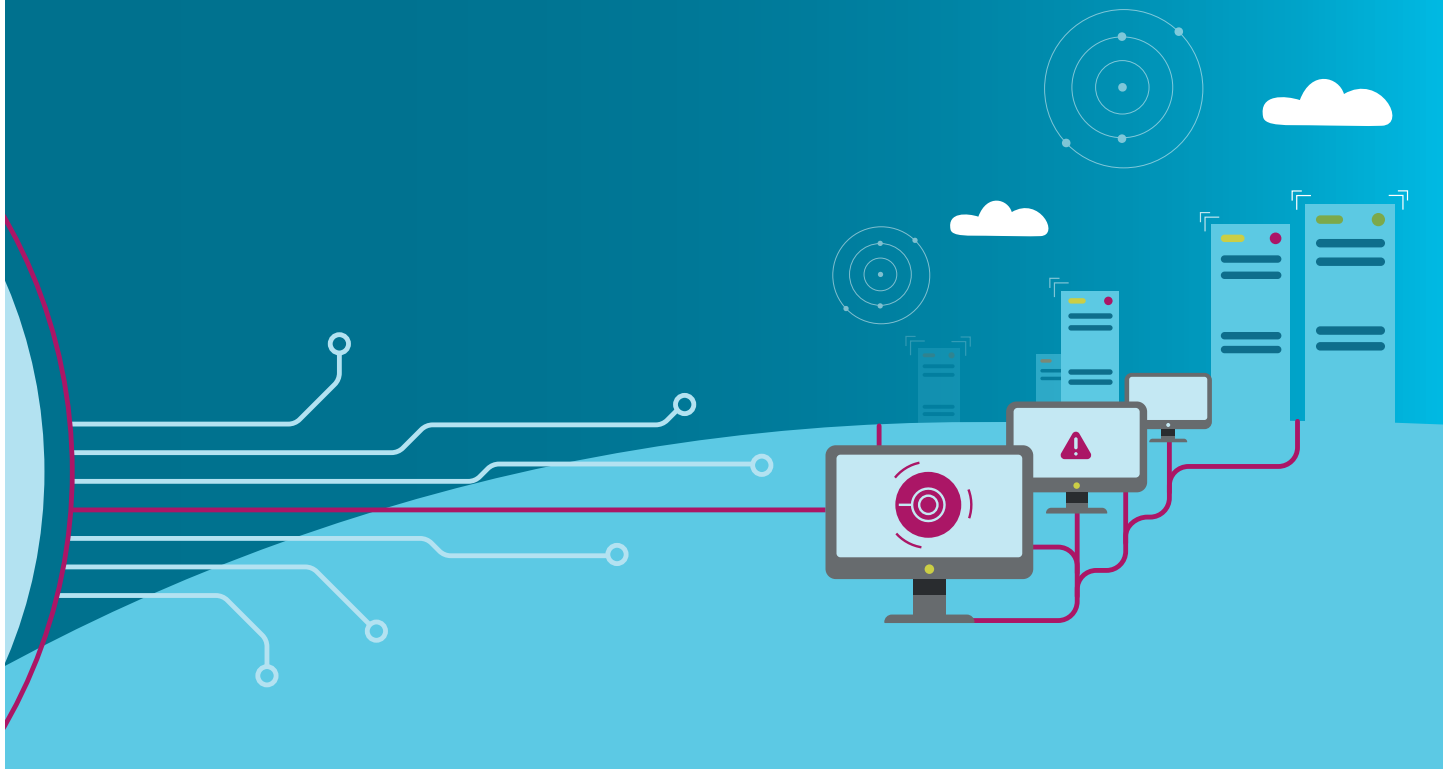


FOCUS

#22 – April 2017

# CYBER RISK ON THE RISE

From intangible threat  
to tangible (re)insurance solutions



The views and statements expressed in this publication are the sole responsibility of the authors.

# CONTENTS

- 5 — CYBER RISKS ARE ON THE RISE  
*Denis Kessler*, Chairman & CEO, SCOR
- 11 — THE CYBERSECURITY  
THREAT LANDSCAPE  
*Bruce McConnell*, Global Vice President, EastWest Institute
- 16 — Summary of the panel discussion on  
NO COUNTRY FOR OLD MEN:  
THE CYBER RISK LANDSCAPE
- 19 — IMPLEMENTING  
CYBERSECURITY  
*Jean-Michel Orozco*, Senior Vice President Head of cybersecurity, DCNS Group
- 23 — STATE OF THE CYBER  
(RE)INSURANCE MARKET  
*Didier PARSOIRE*, CUO, Cyber Solutions, SCOR Global P&C  
*Sébastien HEON*, Deputy CUO, Cyber Solutions, SCOR Global P&C
- 30 — Summary of the panel discussion on  
CYBER RISKS AND INSURANCE FOR CORPORATES:  
A TRUE GLOBAL RISK MANAGEMENT APPROACH  
AND A NEED FOR FURTHER DIALOGUE
- 34 — TECHNOLOGY:  
SHAPING THE RISK LANDSCAPE  
*Victor Peignet*, CEO, SCOR Global P&C
- 41 — Summary of the panel discussion on  
PANEL DISCUSSION  
ON MODELLING AND PRICING CHALLENGES  
*Simon Dejung*, Engineering Underwriter, SCOR Global P&C
- 46 — Summary of the panel discussion on  
AGGREGATION  
AND CLASHES MONITORING  
*Paul Nunn*, Head of Catastrophe Risk Modelling, SCOR Global P&C
- 50 — PROSPECTIVE  
ON DIGITAL INNOVATION  
*Oussama Ammar*, Founder, The Family





# CYBER RISKS ARE ON THE RISE

## Denis Kessler, Chairman & CEO, SCOR



**DENIS KESSLER**  
Chairman & CEO  
SCOR

Denis Kessler, a French citizen, is a graduate of HEC business school (Ecole des Hautes Etudes Commerciales), holds a PhD in economics and advanced degrees in economics and social sciences, and is a Fellow of the French Institute of Actuaries.

He was Chairman of the Fédération Française des Sociétés d'Assurance (FFSA), Senior Executive Vice-President and member of the Executive Committee of the AXA Group and Executive Vice-President of MEDEF (Mouvement des Entreprises de France). He joined SCOR as Chairman and Chief Executive Officer on 4 November 2002. In January 2016, he was elected to join the Academy of Moral and Political Sciences of the Institut de France.

In my view of the risk universe, there are three types of risks: "Acts of God", which relate to natural events, "Acts of men", which are the result of technological progress, and "Acts of the devil", which include crimes, acts of war and terrorist attacks.

The risk universe is expanding, both in terms of complexity and severity. The interactions between the risks are becoming increasingly intricate. Supply chains can be disrupted by circumstances as diverse as floods in Thailand,

the bankruptcy of a shipper, or even the coming to pass of a geopolitical risk.

Cyber risk is a perfect example of how complex risks can be today, as cyber is recent, intangible, invisible, cross-border, and rapidly developing, at a pace with technology. In a cyber context, "Acts of men" include accidental events with unintended damages or consequences, while "Acts of the devil" refer to cybercrime.

## CYBERSPACE IS A MAN-MADE ENVIRONMENT THAT HAS DEEPLY TRANSFORMED OUR SOCIETIES, AND HAS ALSO CREATED NEW RISKS

### IN LESS THAN 60 YEARS, DIGITAL TECHNOLOGIES HAVE DEEPLY TRANSFORMED SOCIETY AND THE ECONOMY

Cyberspace is a man-made environment created in the U.S. in the late 1960s, based on the developments of post-war technology. In the document that describes the Internet Protocol (Berkeley, 1981), security was described as an option that was "unnecessary for the most common communications." Security was not a primary concern back then.

SCOR's headquarters (see figure 1) stands on the site of a bunker that once held Germany's most advanced encryption systems during World War II. All intercepted Allied communications passed through this hub for analysis. After the Liberation, the 805<sup>th</sup> U.S. Army Signals Detachment installed SIGSALY, a 50-ton voice encryption system for direct communication between London and Washington, at this site. SIGSALY is considered to have been the start of the digital revolution.



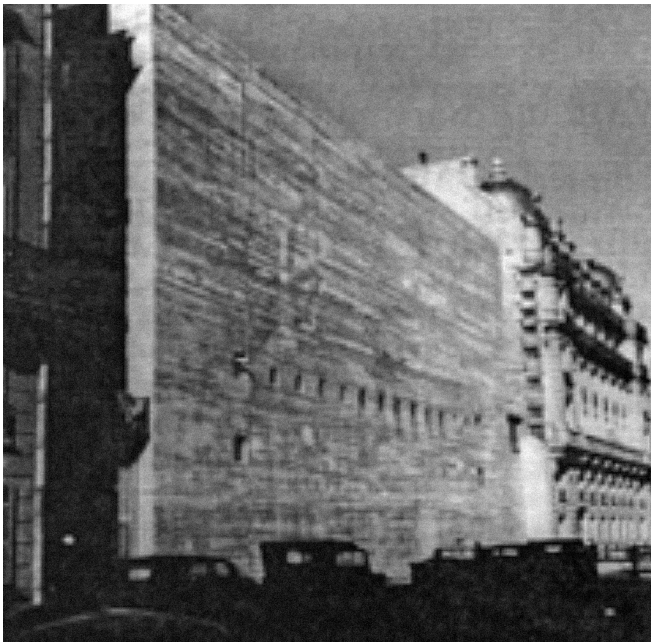


FIGURE 1: SCOR BUILDING IN 1944,  
AND ITS AUDITORIUM WITH A SIGSALY TERMINAL IN 1945

Source: John D. Paul

For reinsurers, viruses are a nightmare, whether they cause epidemics (biological), or cripple operations (digital). The Morris Worm, designed by Robert Morris in 1988, was the first "virus" to spread widely over the Internet and have a significant impact. The program was initially built to hop from one computer to another to assess the size of the Internet, but a coding mistake made it crash the computers it was running on. It infected 10% of the Internet (60,000 computers connected at that time, compared to approximately 10 billion connected devices in 2015<sup>1</sup>). Clean up took days, and the U.S. Government Accountability Office estimated the cost of the damage at USD 100,000–10,000,000.

Originally funded and built by the public sector, cyberspace has been leveraged and massively developed by private companies, with major positive impacts on the economy. In a study published in March last year, the O.E.C.D. recognized the link between the Internet's open, distributed, and interconnected nature and its catalyst role for economic growth and social wellbeing<sup>2</sup>.

Traditional business sectors, like banking, are currently being transformed by digital innovations, and new business sectors have emerged, such as online gaming (market volume of USD 35 billion in 2013, forecast to reach USD 56 billion in 2018<sup>3</sup>).

### PUBLIC AND PRIVATE SECTORS MAY HAVE CONFLICTING INTERESTS

Though operated by private companies, cyberspace is an environment where governments need to have some control. Governance of cyberspace is gradually taking shape, but still lacks maturity, in part because the interests and objectives of governments and those of the private sector are not aligned.

Governments view cyberspace as a trans-border environment where national laws are difficult to apply, and as the limit (or maybe even the end) of the Westphalian sovereignty principle. In addition, there are discrepancies in how governments perceive their roles: the Western approach is based on control and security of infrastructures, while some countries, like China and Russia, exert control over the

1 - Between 8 billion and 16 billion, depending on sources. See for example <http://www.cisco.com/c/en/us/solutions/service-provider/vni-network-traffic-forecast/infographic.html>  
2 - ECONOMIC AND SOCIAL BENEFITS OF INTERNET OPENNESS - 2016 MINISTERIAL MEETING ON THE DIGITAL ECONOMY, O.E.C.D. Report  
3 - <http://www.statista.com/statistics/270728/market-volume-of-online-gaming-worldwide/>



content. Furthermore, governments, while advocating for and promoting cybersecurity, maintain offensive capabilities for intelligence purposes, as demonstrated by Edward Snowden's revelations about the NSA's PRISM program. As a result, international regulations related to cybersecurity have not been widely adopted and are still taking shape.

On the private sector side, there is still insufficient financial incentive to deploy security solutions or standards at a global level. Companies are often reluctant to invest in cybersecurity, because it is perceived as being pure cost with no return on investment. Too often, companies address this problem from an IT standpoint, rather than from an enterprise risk angle. Yet it is essential that cybercrime be brought to the attention of all stakeholders. Furthermore, IT companies are under intense time-to-market pressure to launch new software and digital services. As a result, security, which entails additional costs and delays, may be insufficiently addressed.

## AN ENVIRONMENT THAT FOSTERS MALICE

On the 25<sup>th</sup> of December 2015, the hacking group Phantom Squad launched over 10,000 attacks against the Xbox and PlayStation online networks in the U.S. When asked why they had done it, their response was "Because cybersecurity does not exist."



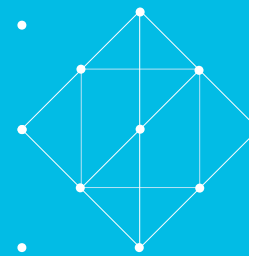
Some malicious actors exploit the many inherent weaknesses of the complex cyber environment, and notably the relative immaturity of cyber defenses, to steal data, to inflict harm or damage and/or illicitly gain profit.

Cybercriminals enjoy relative immunity, for several reasons. There is first an attribution problem: it is almost impossible to gather conclusive evidence connecting a given individual to a cyberattack. Second, it is difficult to bring cybercriminals to court, due to delays in international police cooperation procedures that are not compatible with IT speed, since evidence may be automatically erased after a few days or weeks. Governments may even hire hackers for intelligence purposes, in exchange for protection against prosecutions for cybercrime.

## THE DIGITAL REVOLUTION INCREASES EXPOSURE TO CYBER RISKS

The value of intangible assets is increasing. According to the Global Intangible Financial Tracker 2015, which provides a worldwide review of the world's intangible value, "For rich nations, the value and importance placed on intangible assets, such as brands, people, know-how, relationships and other intellectual property, is now a greater proportion of the total value of most businesses than is the value of tangible assets, such as plants and machinery."<sup>4</sup> As a result, data becomes an increasingly valuable target for hackers.

Cybercrime is bigger than the global black market in marijuana, cocaine and heroin combined (USD 288 billion per year) and approaching the value of all global drug trafficking (USD 411 billion per year)<sup>5</sup>.



The current increase in connected objects and services offers hackers new targets, and the risks will understandably increase as connected objects proliferate. The so-called "Internet of Things" is therefore both a major innovation and a great challenge from a cybersecurity standpoint, all the more since attackers do not only focus on data theft: they may also target a nuclear plant, a car, a plane or even a pacemaker to inflict harm or damage.

This explains the increasing demand for protection and, as with any risk, it is incumbent on insurers and reinsurers to provide solutions to cover it.



4 - [http://www.cimaglobal.com/Documents/Thought\\_leadership\\_docs/reporting/Brand-Finance-GIFT-Report-2015.pdf](http://www.cimaglobal.com/Documents/Thought_leadership_docs/reporting/Brand-Finance-GIFT-Report-2015.pdf)  
5 - Norton Symantec report 2012 - <http://uk.norton.com/cybercrimereport/promo>



# CYBER RISKS ARE BOTH SO PRESENT AND SO UNKNOWN

Characterizing risks is a key concern for a reinsurer like SCOR. However, although they are widely publicized, cyber risks remain difficult to define. Unlike virtually all risks in the context of insurance and reinsurance, they may not be located in the “regular” space and time environment.

## CYBER RISKS ARE RECENT AND ARE DEVELOPING VERY FAST

Cyber risks have only existed for 25 or 30 years. As a result, there is little historical data and no common methodology for defining and assessing cyber events. Nor is there any regular reporting on cyber breaches: unless forced by regulations (e.g. data privacy in the U.S. and the GDPR<sup>6</sup> in Europe in 2018), organizations do not report cyber breaches, because they fear reputational impact and the fact that disclosing vulnerabilities could further attract hackers. Besides, sophisticated cyberattacks are stealthy and difficult to detect: according to cybersecurity provider Protection Group International, 66% of cyberattacks are discovered by external parties, and the median number of days before detection is 229! At this stage, no organization has been empowered to collect, anonymize and build statistics with cyber breach data. Yet insurers and reinsurers need reliable statistics to be able to assess and hence cover risks period. It is therefore critical that available data on cyber incidents be further structured.

Indeed, cyber risks are developing so fast that any data on cyberattacks could become obsolete within months or years of being collected if the process of data collection was not consistent.

## CYBER RISKS ARE PERVASIVE AND MAY HAVE SEVERE IMPACTS

Cyberattacks can disrupt critical infrastructure. In December 2015, there was a blackout in Ukraine after hackers shut down a power station. All the same, a steel plant, suddenly shut down by hackers in 2014 in Germany, suffered in broken furnaces and lost production.

Nobody is immune, almost all organizations – private and public, large and small – use common software, hardware and IT services. The dominant providers have huge market shares: 90% for Microsoft Windows (as of May 2016), 56% for CISCO routers (H1 2016), 31% for Amazon Cloud (H1 2016), and 26% for SAP (as of 2014). While new software comes out with new vulnerabilities every day, old - and therefore vulnerable - software remains accessible.

CYBER HAS CONSEQUENCES ON ALL RISKS AND ALL BUSINESS LINES		
Business interruption	Contingent business interruption	Data and software loss
Cyber ransom and extortion	Intellectual property theft	Incident response cost
Network security	Reputational damage	Regulatory & legal defence costs
Communication and media misuse	Legal protection	Assistance coverage
Claims against directors and officers	Environmental damages	Physical asset damage
Financial theft and/or fraud	Breach of privacy	Bodily injury and death

CRO Forum Concept Paper on a proposed categorization methodology for cyber risk

FIGURE 2: VARIETY OF WAYS IN WHICH CYBER RISK COULD AFFECT BUSINESS LINES

Because of this market concentration and because all networks are interconnected, it is easy to imagine a large-scale, global cyber catastrophe.

Major cyber economic losses have been in the USD 1 billion range, but this is probably far from the worst-case scenario. Indeed, third-party losses have remained very limited so far, with almost no successful class action or individual lawsuits. Furthermore, intangible assets are not valued *per se*, and thus have not yet been widely covered by insurance.

## A CHANGING CYBER CLIMATE: PREPARE FOR MORE “CYBER CATASTROPHES”

Cyber threats are classified among the most serious threats by many nations and international organizations. According to the World Economic Forum (WEF), they are among the top 10 risks in terms of likelihood.

In France, the Secrétariat Général de la Défense et de la Sécurité nationale (SGDSN) lists cyber risks as the second-largest threat to the country’s security<sup>7</sup>, after terrorism but before espionage and organized crime.

6 - General Data Protection Regulation  
7 - [http://www.sgdsn.gouv.fr/site\\_rubrique60.html](http://www.sgdsn.gouv.fr/site_rubrique60.html)





While the importance of this threat is widely recognized, assessing the likelihood of a cyber catastrophe and developing credible cyber catastrophe scenarios to quantify their impacts remains a challenge. According to the WEF,

*“Organizations lack common measures to quantify cyber threats, curtailing the ability to make clear strategic decisions concerning optimal access and investment levels.”*

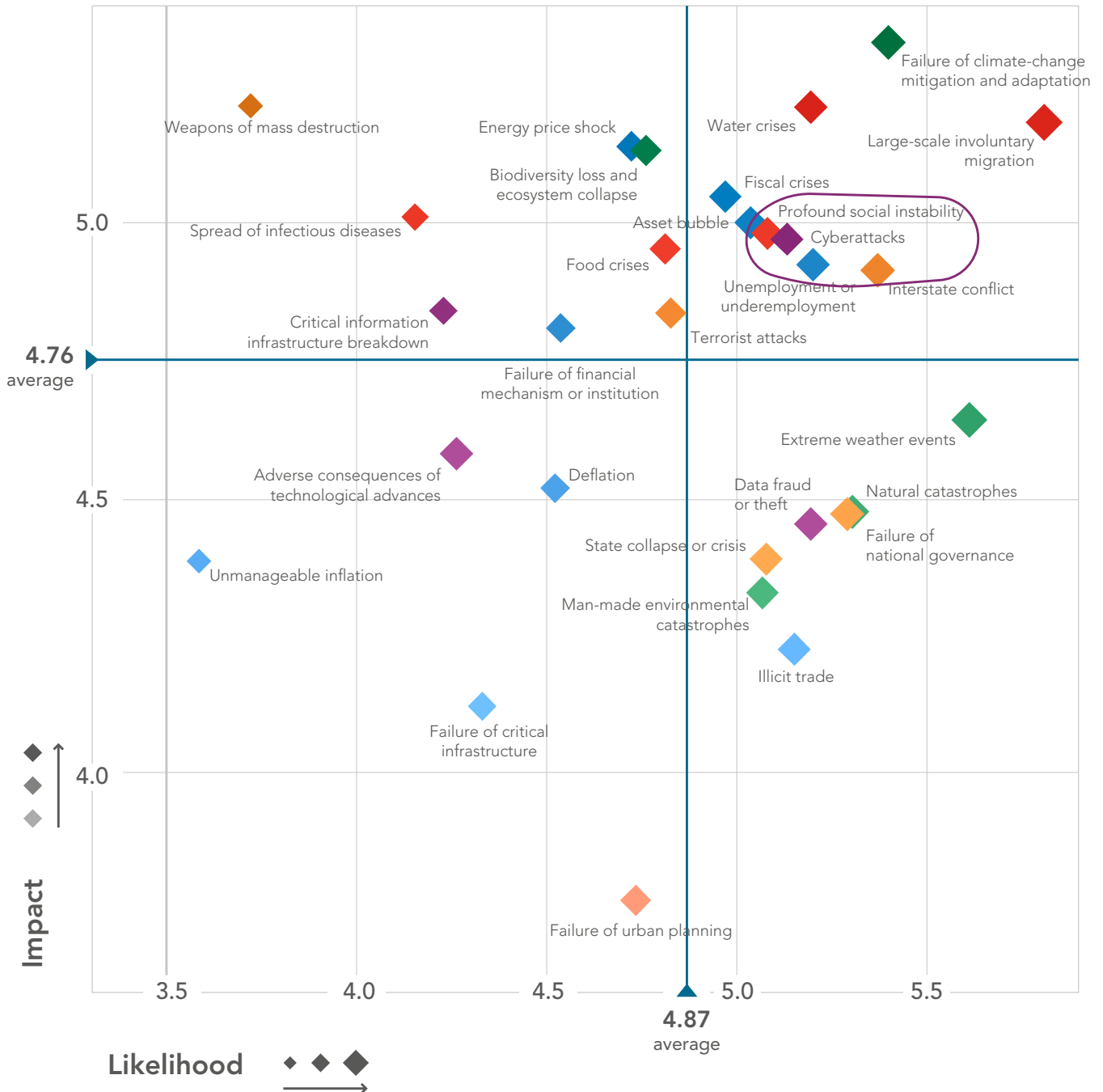


FIGURE 3: LIKELIHOOD AND POSSIBLE IMPACT OF CYBER CATASTROPHES COMPARED TO OTHER RISKS

Source: World Economic Forum Global Risk Report 2016



## HOW SCOR IS ADAPTING TO THE CHALLENGES OF CYBERSPACE

SCOR constantly improves its own cybersecurity. In 2012, SCOR started its major Data Protection Program. The Group has implemented robust cyber protection systems and security tools meeting financial sector standards. In addition to this, SCOR's IT network is continuously monitored by a Security Operations Center under the Chief Information Officer's responsibility.

A cyber risk dashboard that contains all major issues related to cyber risk, including projects, security and compliance, and business opportunities, is shared with the Risk Committee of the Board of Directors on a quarterly basis.

SCOR is further protected by cyber insurance coverage.

Depending on the type of event affecting the Group's data and systems, the insurance program may cover SCOR's own

damages, third-party liability and costs, and services related to crisis management.

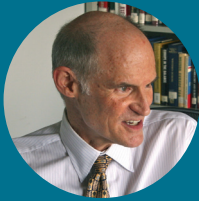
The development of the cyberspace, and its related risks, is creating underwriting opportunities for the insurance and reinsurance market. Even if the market is not yet mature, the cyber risk (re)insurance industry will need to accompany the increased digitization of our societies and is therefore on the verge of significant development. SCOR aims to leverage digitalization to enhance operations and to be a leader in the fast-growing cyber (re)insurance market so as to bring tangible solutions to its clients.

**Denis Kessler Chairman & CEO, SCOR**



# THE CYBERSECURITY THREAT LANDSCAPE

## Bruce McConnell, Global Vice President, EastWest Institute



**BRUCE McCONNELL**  
Global Vice President  
EastWest Institute

McConnell, one of the world's leading experts on cybersecurity, leads the EastWest Institute's Global Cooperation in cyberspace Initiative, working with governments and the private sector worldwide to make cyberspace safer and more secure.

Prior to joining EWI, he served as Deputy Under Secretary for cybersecurity at the U.S. Department of Homeland Security, responsible for ensuring the cybersecurity of all federal civilian agencies and the most critical U.S. infrastructure. Previously, McConnell served on the Obama-Biden Presidential Transition Team, built and sold two consultancies, coordinated international Y2K preparations on behalf of the World Bank and United Nations, and served in the Executive Office of the U.S. President, where he co-chaired the White House interagency working group encryption policy.

## CYBERSECURITY AND THE GEOPOLITICAL THREAT

Three years ago, U.S. National Security Advisor Susan Rice observed that the world's "most vexing security challenges are transnational security threats that transcend borders: climate change, piracy, infectious disease, transnational crime, cybertheft, and the modern-day slavery of human trafficking." To this list, we could add migration, violent extremism, and the safety of fissile nuclear materials.

These issues share at least two characteristics. First, they are accentuated in their severity by modern technology. Second, there are no effective international regimes or institutions that have these problems in hand.

As in other threat domains, we must work towards a more stable environment, a safer ecosystem, reduced risk, and lower potential costs to individuals, firms, and society.

## CYBERSPACE SECURITY AND STABILITY

Global flows of electronic information – financial and business transactions, social media interactions, state-on-state espionage, and criminal activity – strongly resemble maps of a more mature network, the air traffic system.

While there are extensive safeguards in place to keep the air traffic network secure, we have no such safeguards in cyberspace, even though the financial value of the commercial transactions conducted over the Internet (not counting SWIFT and other special-purpose networks) is actually 100 times greater on an annual basis than the value of goods transported in the air cargo system. Commercial aviation has the benefit of public and private organizations that partner to maintain safety and security on a global basis, while there are no comparable institutions for cyberspace. Finally, norms of behavior and international law apply in airspace, but in cyberspace, the applicability of international law is still being debated.

A group of governmental cyber experts at the United Nations has worked for over 10 years to draft an initial set of non-binding norms of behavior in cyberspace:

- ◆ **Not allowing the use** of ICT (Information and Communication Technology) to intentionally damage another country's critical infrastructure
- ◆ **Not allowing international cyberattacks to emanate** from their territory
- ◆ **Responding to requests** for assistance from another country that has been attacked by computers in the first country
- ◆ **Preventing the proliferation** of malicious tools and techniques and the use of harmful hidden functions
- ◆ **Encouraging responsible reporting** of ICT vulnerabilities and sharing associated information
- ◆ **Not harming the information systems** of the authorized cybersecurity incident response teams



## GLOBAL CYBER ARMS RACE

We are experiencing a global cyber arms race led by the United States, Russia, China, Iran, Israel, and some European countries, with many others, including North Korea, following close behind. Non-state actors such as organized crime syndicates and terrorist groups are also a threat.

This arms race differs from the nuclear arms race of the last century. First, the scale of potential damage from even the worst cyberattack is much lower in physical, financial, and human terms. That is the good news. On the other hand, it is much easier to access powerful weapons than it is to assemble a nuclear device, and cybercrime-as-a-service is a vibrant industry. Third, the private sector is much more powerful in cyberspace than in the nuclear space. Major companies have a much greater say in what goes on in cyberspace than most sovereign states. Finally, in cyberspace

there is a much more significant danger of escalation. It is very hard to tell in real time who is responsible for a cyberattack, and relatively easy for a malicious actor to make it appear that an attack is coming from somewhere else.

Some major international companies are working to develop and promote norms of industry behavior:

- ◆ **Creating** more secure products and services
- ◆ **Not enabling states** to weaken the security of commercial, mass-market ICT products and services
- ◆ **Practicing** responsible vulnerability disclosure
- ◆ **Collaborating** to defend customers against and help them recover from serious cyberattacks
- ◆ **Issuing updates** to protect their customers no matter where the customer is located.

---

## ENTERPRISE THREAT

In government circles, security risk is understood to be a function of three components:

- 1/ vulnerability
- 2/ threat, and
- 3/ consequences.

Below, each of these components is examined in terms of the threat to commercial enterprises in the cyberspace context.

### 1/COMPONENTS OF RISK: VULNERABILITY

Vulnerabilities abound in the technology the global economy depends on. A large software program may contain tens of millions of lines of code, each of which may introduce a vulnerability because of uncorrected errors or unanticipated (or, worse, maliciously intended) interactions with other parts of the program. That is why the cybersecurity community refers to interconnected digital technology as the “attack surface.”

In no other industry do customers/users expect and tolerate the level of defects that we experience with supply Information and Communications Technologies (ICT). And then there is the almost complete lack of liability exposure that ICT firms face, particularly in software, and which users perpetuate every time they click “I Accept.”

Clearly, the industry is still immature. Its rapid growth in importance has outstripped systems of governance, including the first line of defense – the market. The market

has given us convenience and efficiency in business and in our private lives. Today, buyers are starting to recognize the criticality of ICT to their daily activities, and thus they demand, and may be willing to pay for, security.

### EVOLVING ATTACK SURFACE

The situation is made more complex due to a dynamic technological environment with product cycles of 18 months or less. There are three major developments that are already affecting the security picture.

#### • VIRTUALIZATION AND THE CLOUD

We are increasingly storing our information in the cloud, on virtual machines operated by major providers like Amazon Cloud Services. This trend has a mixed impact on security. The cloud offers better capacity and capability, and is more resilient. It is easier to ensure security than it is for an enterprise. But it also offers a concentrated target that, if compromised, has greater potential consequences.

#### • THE INTERNET OF EVERYTHING

The Internet of Things (or “of People” or “of Everything”) is another emerging source of risk in cyberspace. By 2020, there will be ten times more devices – such as heart monitors, automobiles, thermostats, machine tools, and floodgates – connected to the Internet than there are phones and computers.

While these devices promise to transform major industries, they will also create a ubiquitous, global sensor network that will know and communicate what is going on everywhere.



These devices will be shockingly insecure; built with easily guessed passwords, transmitting data in the clear, and unmodifiable when vulnerabilities are discovered.

“BY 2020, THERE WILL BE TEN TIMES MORE DEVICES CONNECTED TO THE INTERNET THAN THERE ARE PHONES AND COMPUTERS, AND THESE DEVICES WILL BE SHOCKINGLY INSECURE.”

Although it is generally believed in cyber circles that the Internet of Things represents a massive increase in the attack surface, there is no reason that the “the good guys” should not control the sensor network and use information obtained to increase security.

The Internet of Things may change the way firms invest in cybersecurity. Today firms tend to update every endpoint with the latest security patch and train employees to avoid malware. This is ineffective with 5 billion connected devices, and it will be even less so when there are 50 billion of them. At EWI, we anticipate a shift in strategy, moving away from securing endpoints and towards greater network security within enterprises as well as among cloud service providers and telecommunications companies.

#### • WHAT IS BEING DONE TO REDUCE VULNERABILITY?

Preventing the attacker from getting into most enterprises' systems is impossible at this point. Firms can, however, limit the impact of these vulnerabilities through sound cybersecurity practices.

There are multiple guides available. One that is gaining currency in the U.S. is the cybersecurity Framework created by the National Institute of Standards and Technology (NIST), which is part of the U.S. Department of Commerce. It lays out the basics of a cybersecurity program that all firms should manage to and suggests, depending on their risk preferences, how much security to implement in various areas.

The EWI “Buyers Guide for Secure ICT” is written for firms that want to reduce risk by using safer technology. The guide recommends 25 questions buyers can ask ICT suppliers to help them evaluate the security of the products and services that these suppliers deliver. There are things suppliers can do to reduce the risk of creating vulnerabilities, and these practices are what this guide is intended to encourage.

## 2/COMPONENTS OF RISK: THREAT

Threat is composed of two elements: capability and intent. It is generally agreed that the cyber threat actors who have the capability to carry out mass events and inflict large-scale damage do not have the intent (political, military, economic, commercial, or recreational motives), and that those who would like to disrupt modern life through cyber means do not have the capability. Of course, capability becomes cheaper and more accessible every year, so reassurance is eroding.

Today, the cybercrime-as-a-service industry is booming, and the market in zero days – previously undiscovered vulnerabilities that defenders have no time to prepare for – is robust. Weapons bazaars are hosted on the “dark web” (on servers primarily in Eastern Europe) and attack infrastructures that can infect or disable millions of computers can be rented by the day and paid for with Bitcoins.

Who are these threat actors? In order of decreasing capability they are:

- ◆ States & Proxies
- ◆ Criminal Syndicates
- ◆ Privileged Insiders
- ◆ Non-state Actors including commercial competitors and everyone else

Some states, Russia in particular, use proxies to achieve their offensive goals, including “hacktivists,” who provide a veneer of deniability. State actors may use cyberweapons for conventional purposes, such as economic and national security espionage, or disruption of an adversary’s election. Governments may discover or purchase vulnerability information and stockpile it for future offensive use.

Criminal syndicates use the Internet primarily to fund activities such as human and drug trafficking. The most powerful are located within or near Russia, with a few in Romania. These groups coordinate their activities using the Internet to host highly secure, closed groups that admit members based on trust established in the physical world.

Industrial competitors may use cyber tools to steal proprietary information. Chinese firms stealing from each other is one factor that is driving the Chinese government to fight its own attack activity and start to advocate for better global cybersecurity. Terrorists are non-state actors who use the Internet to propagandize, recruit, educate, and plan. Today, for the most part, they have intent but not capability, at least in terms of cyberspace.

Privileged users (system administrators, for example) do not have a large-scale impact, but can affect companies.



Falling into the “everyone else” category are careless programmers and recreational hackers.

#### Cybercrimes: regular crimes facilitated by the Internet

- ♦ Business interruption Distributed Denial of Service (DDOS)
- ♦ Breaking and entering (for any purpose)
- ♦ Trespassing (for any purpose)
- ♦ Fraud and abuse (for any purpose)
- ♦ Theft (intellectual property and money)
- ♦ Extortion (ransomware)
- ♦ Corruption of data (escalation)
- ♦ Destruction (shutting down an electric grid)

#### COUNTERMEASURES TO REDUCE THREAT

Beyond reducing vulnerability and reducing consequences by having the ability to respond and recover, there are a number of countermeasures to be taken. These include devising cyber norms, deterrents, criminal prosecution, threat of retaliation (the legality of which is much discussed), and attribution. With regard to the latter, it is becoming much easier to identify attackers at a civil level (the preponderance of evidence) and even beyond reasonable doubt in some cases for criminal purposes.

### 3/COMPONENTS OF RISK: CONSEQUENCES

Ironically, it is the rapid increase in the level of possible consequences that is fueling the expansion of the threat landscape. It is much easier and safer to rob a bank online than with a machine gun. The potential damages increase along with our dependency on ICT. If you add to this the aggregation of risk in the form of increasingly large cloud platform providers, and interdependencies and interconnection across sectors, you can come up with some scary scenarios.

---

## RISKS TO INSURERS

The above discussion of vulnerabilities and threats focused on what we know about those elements of risk. But we only know very little about the actual or potential magnitude of the consequences of cyber failures or attacks, which leads to a discussion of the unique risks that the insurance industry faces. From an insurer’s point of view, given our limited knowledge of consequences, we are talking much more about unknown risk than known risk.

Doomsday scenarios like those surrounding the Y2K phenomenon (the Year 2000 Problem also known as the millennium bug) have not materialized, and in fact it is actually quite difficult to inflict broad systemic damage today. But the capability to attempt catastrophic attacks is increasing, and the generally deteriorating international security situation does not help.

---

“THE CAPABILITY TO ATTEMPT CATASTROPHIC ATTACKS IS INCREASING, AND THE GENERALLY DETERIORATING INTERNATIONAL SECURITY SITUATION DOES NOT HELP.”

---

In fact, to date the consequences have been relatively modest. Economic losses from cyberattacks have been estimated to amount to some USD 500 billion every year – less than 1% of the global Gross Domestic Product (GDP) – although the precise figure is not known. In addition to direct financial costs, there are reputational losses and damages to third parties, which is where privacy and data breach laws have focused. But the stock market generally yawns at even the most spectacular attacks.

### AMAZING LACK OF ACTUARIAL DATA

The principal data we have in the U.S. comes from mandatory reports of so-called data breaches, specifically the loss of personally identifiable information. Reporting thresholds vary by state in the U.S., but in general when the theft or inadvertent release of hundreds or thousands of records is detected, firms must report them to state regulators and victims. A fairly mature insurance business has grown



up insuring data-holding companies against the costs of assisting third-party victims. In some cases where there are reporting requirements, the results remain confidential with regulators or reporting is not enforced.

Beyond that, there is limited information to be found in public financial and other reports. The response to a requirement to report material cyber events, levied by the U.S. Securities and Exchange Commission, has produced a few anecdotal reports, but most firms decide the events are not material or comply using very general language.

## LACK OF UNDERWRITING STANDARDS

A second source of risk to insurers is the lack of generally accepted underwriting standards. There is no equivalent to a “building code” for ICT manufacturers. There is no officially recognized independent inspection organization that will certify their products and services. There is no professional licensing of those who write code, nor of those who install and maintain the systems it runs on.

Neither is there an agreed-upon risk management framework. Underwriters are left with a labor-intensive examination of the “security culture” of organizations, or taking a probabilistic approach to policies. One bright spot in the U.S. is the emergence of the NIST cybersecurity Framework as a potential basis for standards. A committee made up of financial services firms has undertaken to adapt the framework to address the specific cybersecurity risks facing exchanges and clearinghouses, and this could become the basis for a standard of care that courts enforce or that regulators adopt.

However, such maturity remains several years away, and the unknowns clearly outnumber the knowns when it comes to assessing cybersecurity risk.

## CONCLUSION

We are facing significant challenges, including increasing capability on the part of malicious actors, a rapidly changing and growing attack surface, a deteriorating international security context, obstacles due to lack of capability or will in the public and private sectors, and – particularly essential to insurers – inadequate standards and information.

Our progress is modest and must be accelerated to make the world a more predictable, and safer, place and in order to prevent major accidental or intentional disruptions to global economic and political stability.





# Summary of the panel discussion on NO COUNTRY FOR OLD MEN: THE CYBER RISK LANDSCAPE

**Frédéric Douzet, Castex Chair of cyber Strategy, Chairwoman and Professor at the French Institute of Geopolitics at Paris VIII University moderated the panel discussion on “No country for old men: the cyber Risk Landscape”.**

The participating speakers were:

- ♦ Ariel E. Levite, Senior Associate at the cyber Policy Initiative, Carnegie Endowment
- ♦ Dr Jason R.C. Nurse, University of Oxford, Research Fellow
- ♦ John Frank, Microsoft, Vice President for EU Government Affairs

There is much more to “cyber” than its technological dimension. Networks are shared among governments, the military, the private sector and civilian society, resulting in complex interactions that are intertwined in cyberspace and difficult to dissociate.



Actions in one area can have consequences in others that are hard to anticipate and not always predictable. Addressing these issues requires that we take a broad view of cyber risks.

## TECHNOLOGICAL TRENDS

In the context of enterprise cyber risk, there are a number of technology trends of particular concern, including the cloud, big data, the Internet of Things, and users and their devices.

We rely on the cloud more heavily each day. In business, cloud services replace or supplement a company’s own servers. In this context, the major risk is third-party data leaks. As companies aggregate greater and greater volumes of data, loss of data, or loss of access to data is a particularly big issue today. If a cloud service provider does not have adequate cybersecurity in place, a company may be adversely affected no matter how strong its in-house security.

The Internet of Things (IoT) is increasing the attack surface considerably. Although it is users – not their gadgets – who are the entry point for most cyberattacks, connected devices

themselves pose a risk of which many organizations are unaware. These devices do not support antivirus software or other types of strong security. Therefore, an organization’s IoT devices could be targets of disruption.

The “smart insider”<sup>1</sup> is an emerging enterprise risk and potentially one of the most significant. This is a malicious or unknowing individual who brings IoT devices into a work setting. There is also the danger of discreet audio and video recording, done intentionally or unintentionally, or discreet backdoor installation. It is essential to understand the complexity of IoT vulnerabilities and to implement appropriate security controls, as well as employee security awareness and training.

1 - Nurse et al., 2015. “Smart insiders: exploring the threat from insiders using the internet-of-things”. In Secure Internet of Things (SIoT). IEEE. <https://doi.org/10.1109/SIoT.2015.10>





---

## GEOPOLITICAL TRENDS

An intense cyber arms race is underway, with a proliferation of capabilities, and a market and tools to support these activities. As revealed by the Snowden disclosures, many governments are actively pursuing offensive cyber capabilities, and widespread data encryption has also led them to spend more time developing sophisticated hacking techniques.

Offensive action by States can contribute to cyber insecurity. Code is left behind after a cyberattack, and the victims can learn from this and retaliate. However, when confronted with a choice between traditional and cyber warfare, the latter may be a more attractive option for States. Such acts could serve a legitimate national security purpose when used – selectively and responsibly – not only for intelligence, but also for offensively targeting equipment in wartime situations. In the current climate, governments must not launch attacks lightly. Several factors could encourage major players to show restraint, including ethical and legal concerns, their own vulnerability to retaliation, the difficulty in accurately identifying foes (misattribution), fear of blowback (systemic effects), and fear of compromising their own capabilities or sources.

While conflicts and crime are increasingly being channeled into cyberspace, States and institutions are weakening. States are under pressure, challenged, and often unable to regulate within their own territories. If States do successfully regulate internally, without international agreement, their rules may be ignored, sidestepped, or interpreted in widely different ways.

There has also been a significant increase in companies offering offensive services to States or corporate clients: those who have significant technological, operational and financial capabilities are developing their skills and offering. These actors are operating in countries where rules are lax and engaging in offensive cyber operations is tolerated.

Perhaps the most serious issues we are facing going forward are the general undermining of confidence and trust, and the manipulation of integrity of data, which is rare, but increasingly worrisome.

---

## A PRIVATE SECTOR PERSPECTIVE

For technology companies like Microsoft, governments are both major customers and Advanced Persistent Threats (APT). Companies must maintain a relationship of trust with governments through transparency and neutrality. It is essential that governments understand that the role of technology providers is not to take sides in the geopolitical debate. Their sole interest in this context should be cyber defense and security.

Governments need to be smarter about procuring information technology, and they need to spend more money to update it. It is also imperative that companies invest in cybersecurity, although certain factors will remain beyond

their control, such as users failing to update or upgrade software. The cloud offers a viable alternative to maintaining and securing in-house IT infrastructure. It can offer significant advantages, such as stronger security models and redundancy.



---

## WHAT SHOULD CYBERSECURITY NORMS COVER, AND WHO SHOULD CREATE THEM?

There are numerous efforts worldwide to establish and implement cybersecurity standards, including the NIST (National Institute of Standards and Technology) cybersecurity Framework in the U.S., and the GDPR (General Data Protection Regulation) in the E.U. Last year, the United Nations Group of Governmental Experts released an important set of norms resembling a cyber code of conduct, which were violated to varying degrees by some signatory countries. However, governments and the private sector should continue efforts to define norms, even though there is no guarantee they will be adopted.

Microsoft issued a draft set of norms for discussion that included a private sector viewpoint because norms produced by governments are invariably skewed heavily towards defense and intelligence. Although it is not the role of private companies to engage in offensive cyber operations, as surrogates for their clients they should participate in discussions of standards and try to build consensus.

One of the biggest obstacles to implementing cybersecurity standards is the costliness of the process and the significant effort required. Another challenge is that, although creating standards is traditionally a governmental task, in the cyber context, multiple stakeholders must contribute their perspectives, which complicates the process.

It may not be practical to define overly specific norms given the volatility of the environment and rapidly changing technology because they could quickly become dated or even counterproductive. Norms must be conceptualized differently, in a way that is tailored to the cyber world in terms of participants, process and substance and other factors.

### BEYOND NORMS: PUBLIC CYBERSECURITY PROGRAMS

Beyond defining norms, governments are implementing programs to increase the cybersecurity of organizations and to assist in the aftermath of attacks. Governments are offering incentives to companies to beef up their security, or assisting them in doing so. In the U.K., for example, the government strongly encourages businesses to participate in the cyber Essentials program, which helps them put in place a minimum number of security measures. A number of insurance companies are currently using the cyber Essentials certificate as a criterion for coverage.

In other countries, governments have put in place mechanisms whereby certain organizations can call on outside Computer Emergency Response Teams (CERT) to assist with response or mitigation if they believe they have been attacked by a state.

---

## WHAT ROLE FOR THE INSURANCE INDUSTRY?

The risks of aggregation in the cyber context are serious and multiple, and we have yet to even grasp their nature. This presents an unprecedented challenge, but the insurance industry is in a unique position to create standards and achieve harmonization. If the industry were to create a sort of Active Defense framework for the private sector, it could be an effective way to approach aggregation risks, while at the same time producing a set of standards that governments could embrace. It might also be beneficial to find a way for governments and the private sector to share responsibility and liability for cyberattacks.

The insurance industry may, in fact, have more power to shift the balance towards security than any other group. In the very dynamic cyber context, in which the current set of problems and solutions will necessarily change, the insurance industry nonetheless has the opportunity to constrain or encourage clients, or to provide incentives to make them take cybersecurity much more seriously. Working with customers to make them more secure will be a continuous process in which insurers will play a very important role.



# IMPLEMENTING CYBERSECURITY

## Jean-Michel Orozco, Senior Vice President Head of cybersecurity, DCNS Group



### JEAN-MICHEL OROZCO

Senior Vice President  
Head of cybersecurity  
DCNS Group



**Jean-Michel Orozco is Senior Vice President Head of cybersecurity of DCNS group. He is responsible for defining and implementing the cybersecurity strategy for the whole group perimeter, from internal IT to industrial and operational IT (products & services).**

Before DCNS, Jean-Michel was CEO of AIRBUS cybersecurity, the AIRBUS subsidiary specialized in providing cybersecurity products and services in Europe. He managed to bring this company in a leading position in Europe with more than 600 cybersecurity experts based in France, UK and Germany. All along his career, Jean-Michel held senior management positions in MATRA and EADS groups and was exposed to a wide range of activities from engineering, large scale program management, sales & marketing and general management. He is a graduate from Telecom Paristech, a French management & engineering school, and from the National Defense University in Washington D.C where he studied geo-strategy, political sciences and international relations.

Cybersecurity is now one of the most important challenges of our modern society. It is a major concern in economic terms, as well as a tremendous threat to national security due to the potentially devastating effects of massive cyber-attack on critical infrastructure. Indeed, our very way of life may be at stake.

The financial value of modern companies is increasingly based on intangible assets. According to "Fortune" magazine, such assets now represent 80% of companies' value. This is a substantial figure, and these assets need to be secure.

"INTANGIBLE ASSETS  
REPRESENT 80% OF  
COMPANIES' VALUE."

80%

This article examines cyber threat in terms of three main categories: espionage, sabotage (achieved through cyberattacks), and cybercrime. It also provides recommendations for establishing cybersecurity measures in corporate organizations.

## CYBER THREATS

### ESPIONAGE

This is a discussion of economic, rather than state-sponsored espionage. Every day, with extraordinary stealth, cybercriminals carry out large-scale economic espionage to undermine the competitiveness of companies. These attackers, who come from a wide range of origins, infiltrate IT and communication networks to steal important or vital company information.

They often start to lay the groundwork for their attacks with social engineering, which is manipulating or tricking people into revealing information or performing some action. They have access to people and a great deal of information that is freely available online, particularly through professional social networks like LinkedIn. On such sites they can obtain information on strategic projects, employee responsibilities, technologies used, and identify vulnerabilities they can exploit.



They then enter the IT system by exploiting vulnerabilities on network. Once inside, they lie low, expand, find the servers and targets they are seeking. When they are ready, they begin exfiltrating data.

“MORE THAN 70% OF LARGE COMPANIES ARE REGULARLY THE TARGETS OF INTRUSION ATTEMPTS. IT IS POSSIBLE THE REMAINING 30% ARE TOO, WITHOUT EVEN KNOWING IT.”



## SABOTAGE

Acts of sabotage can constitute acts of war or terrorism, and this is the case in an international security context. However, it is easier to attack Critical National Infrastructure (CNI), such as mass transport, banking systems and power grids, than it is to attack military targets. An attack on CNI could have devastating effects. The consequences of the shutdown of a national power grid or water distribution system would be dire: beyond the economic impact, there would also be loss of life.

The first such attack probably occurred in 2007, when Russia targeted the Estonian banking system. Later the Stuxnet virus was used against Iranian nuclear enrichment facilities. More recently, France's television network TV5 was the victim of a costly and debilitating attack. Although there have been relatively few attacks of this kind, the risk of facing a "cyber-Pearl Harbor" – to quote former U.S. Defense Secretary, Leon Panetta – is probably increasing daily.

It is interesting to note that cyber warfare is unique in its asymmetry. Unlike in traditional warfare, which requires tens of thousands of troops, a cyberattack requires a relative handful of people. This new asymmetric kind of warfare is the perfect tool to do damage to the strong. In a certain sense it is changing the balance of power all over the planet.

In terms of *modus operandi*, cyber saboteurs use the same techniques as those engaged in espionage, with one difference: the timing of the execution. In a sabotage context, attackers install logic bombs that remain dormant until they are activated. This is the most effective way to synchronize different simultaneous attacks, on different systems, for massive impact and total surprise.

## CYBERCRIME

This type of cyberattack is the domain of organized crime syndicates. Until recently, most cybercrime focused on banking systems and financial institutions. One recent example of this is the attack on the SWIFT (Society for Worldwide Interbank Financial Telecommunication) network, during which attackers attempted to steal nearly USD 1 billion through fraudulent funds transfers.

Organized crime has recently begun using ransomware to extort money from companies and organizations. Ransomware is malware that encrypts the data on a computer or system. Cybercriminals then demand money before they will provide the victim with a decryption key to decrypt the data. The more money a company makes, the higher the ransom. In one recent example, a hospital in the U.S. chose to pay the ransom after one day of non-operation. In another, a shipping company paid the ransom after attackers took control of a ship's machinery, making it impossible to unload its cargo.





# RECOMMENDATIONS TO IMPLEMENT CYBERSECURITY IN A CORPORATE ORGANIZATION

## WHO SHOULD BE IN CHARGE?

In corporate organizations, it is important to emphasize that attackers target not only IT systems, but also companies' products and services. This means that every facet of a company and all of its assets must be considered in the context of cyber risk. Far too often, management thinks of cybersecurity in terms of its IT system alone, neglecting to include products and services, or production and maintenance facilities.

Consequently, it is often the case that the Chief Cyber Security Officer (CCSO) – when there is one at all – is the Chief Information Officer (CIO) himself, or someone attached to the CIO. This is not ideal because CIOs are neither *competent* nor *dedicated*. They are not competent in the sense that they are limited by the constraints of a company's organizational design, being responsible only for the primary IT system. Only sometimes are they responsible for the industrial IT systems, and never for the operational IT systems, those that are embedded in a company's products and services. CIOs cannot be dedicated in the sense that they are continually under heavy budgetary pressure and not generally eager to take on anything that may create an additional financial burden. In addition, they have a natural tendency to prioritize those things that are immediately visible to top management. Unfortunately, good cybersecurity is something that people do not usually see or hear about.

The ideal situation is to have someone in charge of cybersecurity for all facets of a company at the highest level of the organization. This results in a coherent and comprehensive approach to cybersecurity. The CCSO can be a member of the executive board, or a dedicated person reporting directly to the CEO, depending on the nature of the company's business and the complexity of its cybersecurity issues. Companies whose entire business is linked to IT and new technology can probably find a qualified board member. Others should probably choose the second option.

Having the CCSO at the executive committee or senior management level offers numerous key advantages. It sends a clear signal to the entire organization that cybersecurity matters. This is key because the cyber efficiency of a company is highly dependent on employees. A CCSO at this level has considerable independence, a global view and the real power to make things happen. Finally, this person is in the perfect position to educate all executive committee members, which is essential to ensuring the adoption of a culture of cybersecurity throughout a company.

Not having the support of executive committee members can be very detrimental.

“HAVING THE CCSO AT THE EXECUTIVE COMMITTEE OR SENIOR MANAGEMENT LEVEL SENDS A CLEAR SIGNAL TO THE ENTIRE ORGANIZATION THAT CYBERSECURITY MATTERS. IN ADDITION, THIS PERSON IS IN THE PERFECT POSITION TO EDUCATE ALL EXECUTIVE COMMITTEE MEMBERS, WHICH IS ESSENTIAL TO ENSURING THE ADOPTION OF A CULTURE OF CYBERSECURITY THROUGHOUT A COMPANY.”

## WHAT RISKS, WHAT STRATEGY AND WHAT ORGANIZATION?

Once the CCSO is in place, his first tasks should be to define overall cybersecurity needs for the whole group, as well as to implement efficient governance and organization. To properly devise a cybersecurity strategy, the first consideration must be risk, which requires that you understand and are able to characterize the kind of threat you are facing. It might be espionage, sabotage, cybercrime, or some combination of the three. It is important to know whether your attackers are likely to be organized crime, terrorists, or government secret services because it is not the same techniques to defend against these different malicious actors. It is also important to understand the different courses of action attackers might use, their possible targets, and what an attack would mean in terms of business consequences. This process must be undertaken by a multidisciplinary team that includes IT specialists, cybersecurity specialists, people responsible for the company's business, production, maintenance, etc. At this point only, it is possible to prioritize actions, allocate resources, and define top-down priorities.



## WHAT GOVERNANCE?

The next step is defining a principle of governance. Cybersecurity involves multiple people who all contribute to security. Beyond senior management, those who work in design, production, maintenance, support positions, finance and audit, buyers (to see to the cybersecurity of the supply chain), communications (in case of an event your messaging is critical), human resources (to train employees and raise awareness) have to be involved as well. They all contribute, depending on their responsibilities and expected tasks. Finally, it is recommended that the person in charge of implementing the cybersecurity program not be the same as the person in charge of verification and qualification.

## WHAT RESOURCES?

Once the strategy and governance are defined, it is important to ensure that all resources are in place, in terms of both quantity and quality. For a good cybersecurity structure, at the minimum you should consider having a surveillance system, a secured operations center to monitor and detect intrusion activities, teams of incident responders and forensics experts in case of attack, and a threat intelligence unit to make sure you are well informed of evolving threats. Being one step ahead matters in this race against

the bad guys. If the company is big enough, this structure can be implemented in house. Smaller companies can use external service providers. A word of warning: if you wait until a security event happens before putting this structure in place, it will be too late.

## WHAT FRAMEWORK?

The final point concerns measuring maturity level and progress. You should consider defining a company cybersecurity framework, which will serve as an internal point of reference. This will enable you to compare yourself against other companies and measure your level of maturity and progress against recognized standards. You can create a framework yourself, but it is best to build on existing standards, like the "cybersecurity Framework for improving critical infrastructure" created by The National Institute of Standards and Technology (NIST). Once again, your framework should encompass all facets of your business: internal, industrial and operational IT. It should be closely linked to your business management system. With a framework in place, you can regularly assess the way you function, benchmark yourself and identify how to progress. It will help you maintain state-of-the-art protection. Lastly, because there is no such thing as "zero risk," the final step is to cover residual risk through insurance products.

---

## CONCLUSION

It is clear that insurance companies have a major role to play in cybersecurity, not only because of the risk coverage they may provide, but also because of the catalyst effect they will have. It is understandable that insurance companies may be reluctant to commit without knowing how to judge a

customer's defensive preparedness. Yet perhaps this chapter has provided some starting points and standards by which to judge insurance clients' readiness in terms of cybersecurity.



# STATE OF THE CYBER (RE)INSURANCE MARKET

**Didier PARSOIRE, CUO, Cyber Solutions, SCOR Global P&C**  
**Sébastien HEON, Deputy CUO, Cyber Solutions,**  
**SCOR Global P&C**



**DIDIER PARSOIRE**  
 CUO Cyber Solutions  
 SCOR Global P&C



**Didier Parsoire is currently Head of Cyber Solutions, managing the development of SCOR Global P&C cyber Insurance and Reinsurance business. He is also Chief Underwriting Officer of SCOR Global P&C Space Specialty line.**

Beginning his career as Space engineer, he joined SCOR in 1992 as Space Underwriter, taking over responsibility for the Space Department a few years later. Didier also had various managerial positions in the field of Large Corporate Risks from New Tech clients to Captives and Structured Solutions. More recently, he designed an innovative and advanced system for large risk Underwriting before taking the head of SCOR Global P&C Cyber Operations in 2014. Didier Parsoire is a graduate in Aeronautics & Space Engineering from Supaero ("Ecole Nationale Supérieure de l'Aéronautique et de l'Espace").



**SÉBASTIEN HEON**  
 Deputy CUO Cyber Solutions  
 SCOR Global P&C



**Sébastien Héon began his career as math professor and crypto expert for the French Ministry of Defence. After 10 years in various positions in the MoD, he is appointed as Director of International Relations at the French Network and Information Security Agency (ANSSI).**

Sébastien joined Airbus in 2009 as a senior adviser for Intelligence & cyberdefence, and headed the cybersecurity consulting & training division. In this position, he advised decision makers on cyber threats and mitigation of cyber risks. Since 2005, he also has been an associated professor at Paris VII University, teaching cryptology and protocol security to postgraduate students. Sébastien joined SCOR in July 2015 as cyber expert to support the development of the newly created Cyber Solutions unit.

This chapter focuses on how the burgeoning cyber (re)insurance market is developing and the shape it is taking, as well as trends, challenges and key drivers for its development.

## CYBER THREATS: PANORAMA AND TRENDS

Cyber risks encompass a variety of impacts and threat actors that have been segmented in 6 categories (see figure 1). In the last 18 months, all types of cyberattacks have significantly increased. This might be due to two main factors:

the expansion of connected devices that provide attackers with new opportunities and, simultaneously, defenses that become increasingly difficult to implement due to the expanding complexity of IT networks.

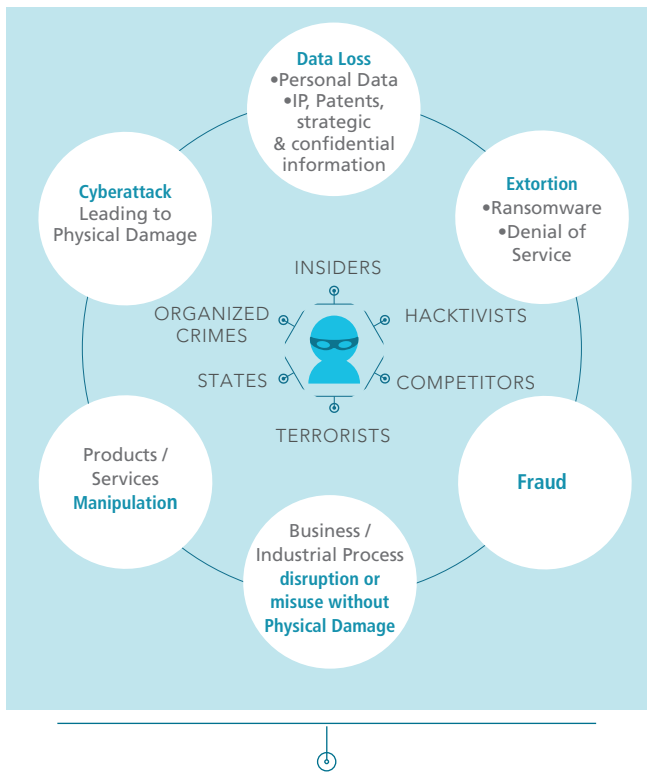


FIGURE 1: CYBER THREATS ENCOMPASS MANY DIFFERENT CASES, TYPES OF LOSS AND MOTIVES

Source: SCOR

## DATA LOSS

Data loss remains the most common case of cyberattack impacting all organizations globally. Malicious actors are usually after personal information (personally identifiable information (PII)), protected health information (PHI), payment card information (PCI), login credentials and passwords, etc.), or companies' strategic, confidential information (mergers and acquisitions (M&A), intellectual property (IP), financial statements, etc.). These sensitive information are then resold on the black market.

In the U.S., there are regulations that require organizations to report data loss and notify users. They are useful in that they provide information on frequency and severity of data breaches.

## CYBER EXTORTION, RANSOMWARE

Ransomware are malicious software that penetrate an IT network and encrypts all available information. The attacker then asks for a ransom, usually in crypto-currency, in exchange to the decryption of data. This model represents pure profit for attackers since they do not have to resell stolen data on the black market. There has been a massive, 300% increase in successful ransomware attacks in the last year. Hospitals as well as universities have been massively hit by this kind of attack with ransoms varying from around USD 100 for individuals up to USD 20,000 for enterprises, and the amounts are rising.

According to the F.B.I., there were nearly 250 cases reported in 2015 for a total of USD 24 million in losses.

## "FAKE CEO" FRAUD

In this case, the attacker impersonates the CEO of company and calls employees to ask them to urgently transfer money to an external bank account, pretending it is for an urgent and secret M&A discussion. This is only peripherally a cyber threat, in that it involves emails and/or calls, but it is included here because it has been mentioned in the context of cyber insurance, and the losses can be significant. In the highest-profile cases, it has resulted in tens of millions in losses: EUR 41,9 million at FACC, an Austria-based aerospace parts manufacturer, and EUR 40,000 at Leoni AG, a cable manufacturer.

## BUSINESS/INDUSTRIAL PROCESS DISRUPTION OR MISUSE WITHOUT PHYSICAL DAMAGE

Business disruption without physical damage is a unique characteristic of cyber risks. For example, Distributed Denial of Service (DDoS) attacks can stop or interrupt the functioning of an IT network by saturating it with a tsunami of data. DDoS attacks have risen 129% in the last year and, in recent months, there have even been 12 "mega attacks".

The impact of business disruption through a cyberattack is similar to business interruption due to other perils and can lead to significant losses. The sophisticated cyberattack that generated a black-out in Ukraine in December 2014 is a good example of this type of disruption.

## PRODUCTS AND SERVICES MANIPULATION

This kind of attack, which focuses on equipment common to many companies or industries, is probably more significant in its potential to cause problems in the future. In the case of SWIFT (banking) and Cisco (routers, firewalls), the attacks were stealthily carried out by people implementing backdoors in devices to bypass security or stealing valid credentials to gain access to sensitive networks.

Attackers of this type are highly motivated, talented, and organized. They design and create malware specific to devices they want to target, manipulating everyday IT operations. The attacks themselves are also carefully planned, starting during weekends when there are few people in the office to respond, for example.

In the case of the SWIFT network, attackers who had log in information implemented malware that could not only transfer money, but also delete the acknowledgements sent automatically as a verification step, thus authorizing all funds transfers. The malware was ultimately detected due to a spelling mistake – a misspelling of the name of a bank – rather than a coding mistake.





In the case of MICROS cash registers (an Oracle subsidiary) attackers got in during the manufacturing and design process, implementing malware that shipped with product. This malware then stole data when credit cards were swiped.



## CYBERATTACK LEADING TO PHYSICAL DAMAGE

This type of threat is also worrying, and we have several recent examples to cite, including attacks against a steel factory in Germany and against Aramco in Saudi Arabia. In Germany, the attackers gained access to the industrial control system of a steel mill and suddenly stopped the furnaces making them break. The more devices there are connected to the Internet, the more probable this type of attacks will be.



## THE REGULATORY LANDSCAPE

One of the main issue of cyber Risk is that we lack standard definition: see figure 2 for some example of definition.

ORGANIZATION	DEFINITION OF IT/CYBER RISK
<b>ISACA</b> Information Systems Audit and Control Association	IT risk is the business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise
<b>IUA</b> International Underwriting Association	Cyber risk [...] essentially encompasses any risk arising out of the use of technology and data
<b>IMIA</b> International Association of Engineering Insurers	Risks arising from the storage, use, computation, and/or transmission of electronic data. Such cyber risks may be malicious, for example caused by individual hackers or nation states, or inadvertent, for example caused by a coding error.
<b>Chief Risk Officer (CRO) Forum</b>	The definition of cyber risk covers : <ul style="list-style-type: none"> <li>♦ Any risk emanating from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks</li> <li>♦ Physical damage that can be caused by cyberattacks</li> <li>♦ Fraud committed by misuse of data</li> <li>♦ Any liability arising from data use, storage and transfer</li> <li>♦ The availability, integrity and confidentiality of electronic information, be it related to individuals, companies of governments</li> </ul>



FIGURE 2: CYBER RISK HAS NO STANDARD DEFINITION

Cybersecurity researcher Bruce Schneider recently said that over the past year or two, someone has been probing the defenses of companies that run critical pieces of the Internet. These probes take the form of precisely calibrated attacks that serve to determine how strong those companies' defenses are. We must explore credible scenarios in anticipation of the possibility that attackers may one day breach these defenses.

However we now see the regulatory landscape evolving quickly (see figure 3). In the U.S., there are regulations requiring companies to report data breaches and notify customers. Last year, a bill was introduced in the U.S. with the aim of standardizing fragmented regulations per sector and per state, and proposing a unified definition of what constitutes personal information.

The E.U. is still operating under the 1995 European Data Protection Directive, but this will be superseded by the General Data Protection Regulation (GDPR) in May 2018. This will likely be a very positive development for the protection of private data in the E.U. The GDPR will be quite similar to regulations in the U.S., which have been a significant driver for the growth of the cyber insurance industry there.

"IN 2018, THE EUROPEAN GDPR WILL BE QUITE SIMILAR TO REGULATIONS IN THE U.S., WHICH HAVE BEEN A SIGNIFICANT DRIVER FOR THE GROWTH OF THE CYBER INSURANCE INDUSTRY THERE."

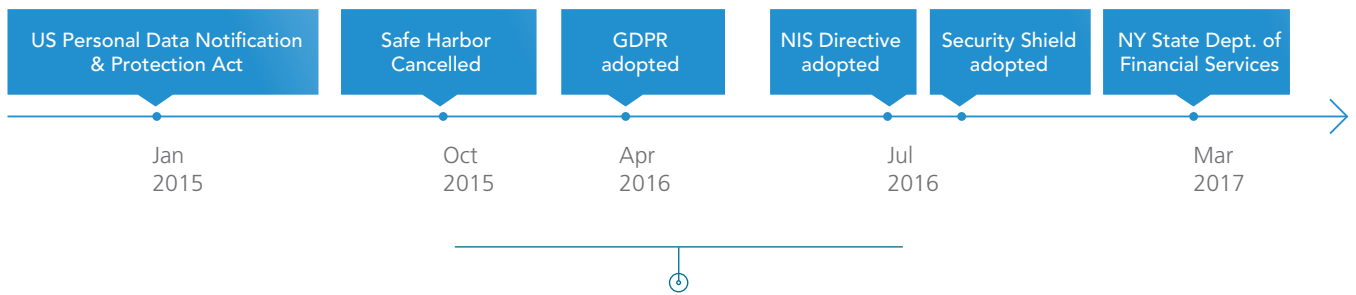


FIGURE 3: EVOLUTION OF RECENT CYBER REGULATION

Source: SCOR

The new Directive on Security of Network and Information Systems (NIS Directive) is designed to protect critical infrastructure in the E.U. by requiring operators of such infrastructure to implement cybersecurity measures and

to notify public authorities of major cyber incidents. This reporting requirement should enable the collection of data, which could be used by the insurance market.

## OVERVIEW OF CYBER INSURANCE PRODUCTS

Cyber-specific policies usually provide two main groups of guarantees:

- ♦ **First-party coverages** such as costs of recollection, restoration or rebuilding of lost data, cyber extortion, fraud and business interruption (without material damage) following a cyber event.
- ♦ **Third-party coverages** including privacy liability arising out of the loss or theft of 3<sup>rd</sup> party data, liability for any damage caused to third parties due to misuse or breach of security of a company's IT system as well as Internet media liability.

These coverages are packaged with a set of guarantees compensating the expenses incurred to manage the cyber event such as Forensic and investigation costs, Public Relation costs, notification or assistance to the individuals subject to breach of personal data and regulatory inquiries that may entail defense costs and penalties

Besides cyber-specific coverages, cyber events may also trigger traditional Policies providing no explicit cyber cover, bringing additional exposure in the insurer's portfolios through the so-called "silent cover". This includes first-party policies such as property, construction/erection all risks (CAR/EAR) or crime, as well as third-party policies such as General Liability, Errors and Omissions (E&O), Professional Indemnity, Directors and Officers (D&O) (see representation in figure 4).

Property policies generally have a cyber exclusion removing exposure to pure loss of data or IT network and resulting business interruption. However, fire or explosion caused

by a cyberattack would be covered. On the liability side, we usually don't find any cyber-specific exclusion and most policies would respond to the extent that the loss falls within the scope of coverage. For example, a company's general or product liability policy may indemnify bodily injury caused by a cyberattack.

### THE CYBER COVERAGE LANDSCAPE

When it comes to purchasing cyber insurance, we see a full spectrum of purchasing behavior from clients, and trends show that clients are keen to increase their level of coverage.

Minimum coverage generally entails removing the cyber exclusion from a property policy. Because property policies are usually all-risk policies, depending on the policy terms, insurers may end up paying in case of data loss or business interruption without material damage.

A second level of coverage can be provided through affirmative cover given by coverage extensions or endorsements to standard policies.

Data restoration costs or business interruption without physical loss can be granted this way in Property policies, though generally sub-limited.

Cyber endorsements can be applied to existing casualty policies, which would provide, for example, explicit cover for breach notification or event management costs. Customers who purchase such minimum coverage may be inadequately covered.

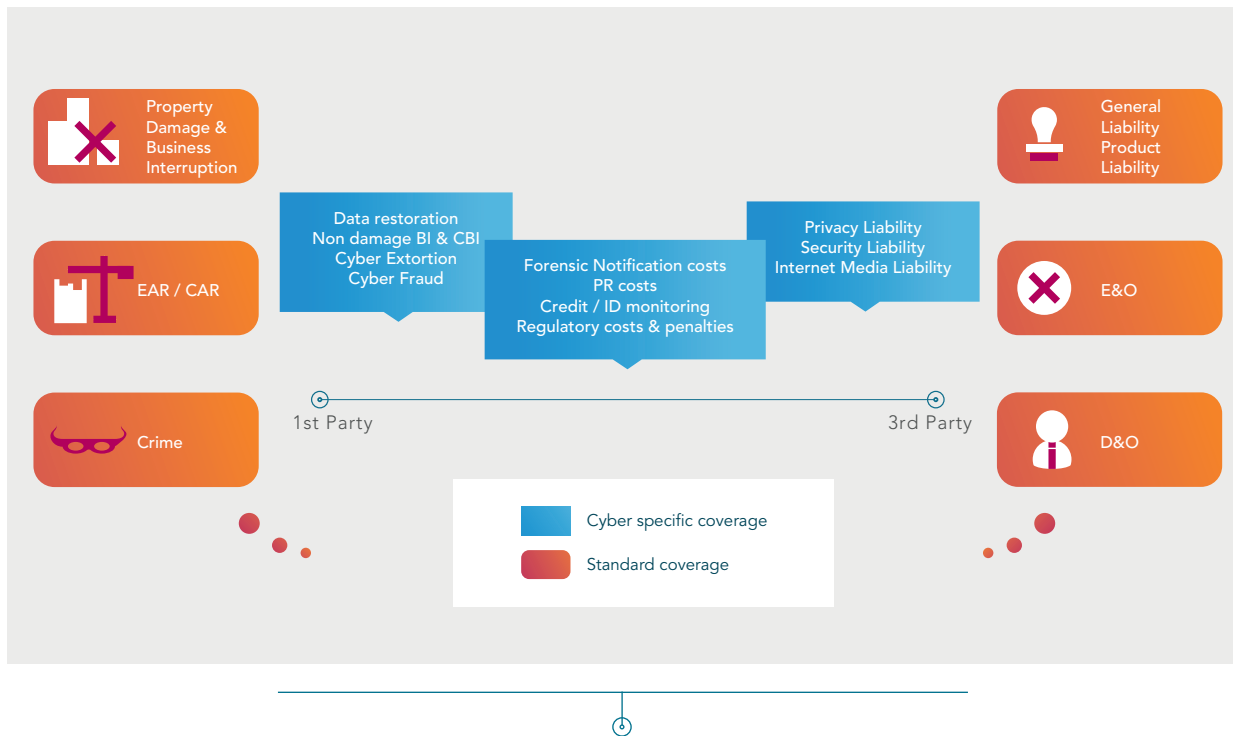


FIGURE 4: A WIDE RANGE OF COVERAGE POSSIBLY RESPONDING TO CYBER EVENTS

Source: SCOR

The most common coverage purchased is what we refer to as a cyber standalone policy, which covers all or some of the circumstances shown below, see below figure 5. Quite often, cyber-specific coverage can be bundled with E&O, which is common for technology companies (a bundled cyber and tech E&O policy).

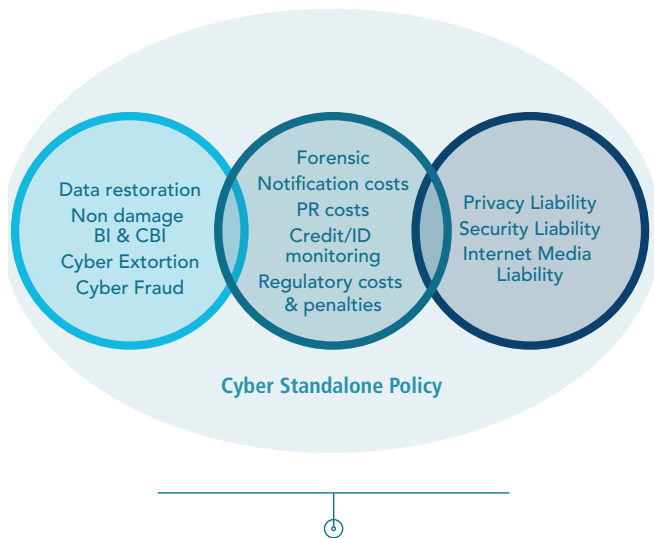


FIGURE 5: CYBER STANDALONE INSURANCE

Source: SCOR

Recently we are seeing a trend towards more comprehensive policies that includes not only cyber-specific coverages,

but also property and general liability coverages being purchased that are specifically intended to cover cyber perils.

While this trend may be seen positively as it tends to clarify where cyber exposure lies across the full spectrum of insurance products, it requires some wording adjustments to avoid overlaps between cyber and existing Standard policies.

### A DIFFERENT PERSPECTIVE ON CYBER INSURANCE

Cyber-specific insurance is not unique as a product. It covers losses that exhibit similar patterns to certain others covered by standard insurance. Indemnification for data loss notification or event management is not that different from the product recall coverage that might exist as an extension in some product liability policies. Cyber extortion is not dissimilar to kidnap and ransom in terms of indemnification process and service provided to the insured. Computer fraud could be covered by a crime or fraud policy.

The indemnification principle for Business process disruption due to an IT network interruption is similar to the one for Business Interruption following a property damage. Data or computer restoration costs are not unlike replacement costs of any asset covered by a property policy. Privacy or Security liability claims are substantially similar to an E&O claim.



Therefore, we suggest considering cyber not so much as a product, but more as a peril. This helps us come up with the right questions raised to the insurance market.

“WE SUGGEST CONSIDERING CYBER NOT SO MUCH AS A PRODUCT, BUT MORE AS A PERIL.”

First, cyber risks are strongly linked to intangible assets, which represent a growing portion of every company's assets. For this reason, the insurance market must focus more on how to value and insure data and intellectual property, and how to quantify reputation damage and determine whether or not it can be insured.

Second, non-physical losses are commonly covered, but we must ensure that the industry has the expertise to indemnify business interruption due to a cyberattack without material damage. We must also face conflicting interests that may exist between criminal investigation and preservation of evidence on one hand and prompt business recovery on the other hand.

Third, we must be ready to cope with the very dynamic threat landscape in which risks are not only increasing, but also changing in nature. This includes increasingly pervasive technology. With connected objects, cyber risk is now entering the physical world, and attacks may result in material damage, bodily injury, and circumstances that are currently covered by existing policies. We need to examine whether standard policies are able to respond to this risk.

Finally, systemic risk is a key issue and risk propagation is an intrinsic feature of cyber risks developing in an interconnected world. We must explore how to manage the accumulation of risk due to common vulnerabilities or cascading effects.

## MARKET FIGURES AND OUTLOOK

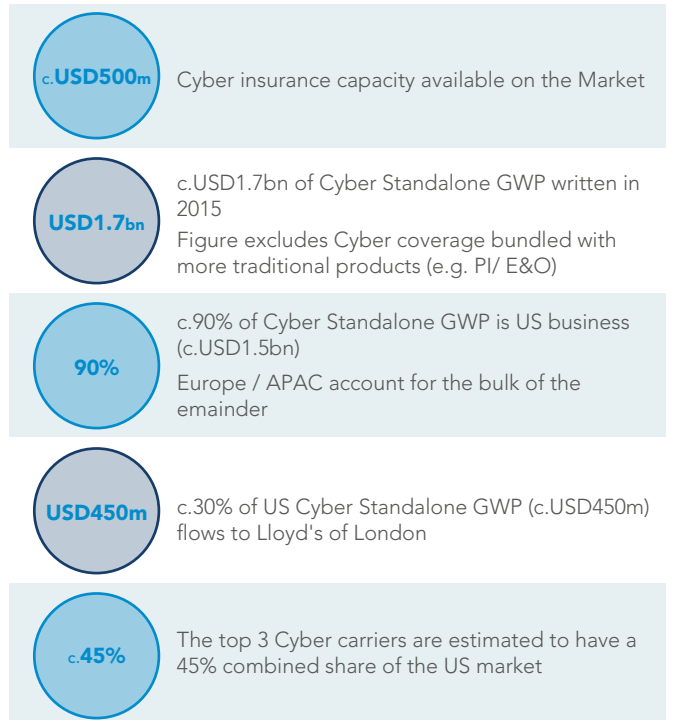
If we consider both cyber standalone and bundled coverage, the Gross Written Premium (GWP) in 2015 was estimated at USD 2.5 billion. By 2020, it is anticipated that the GWP could reach USD 9 to USD 10 billion. This represents tripled growth, a rate that is not being experienced in many classes of the insurance industry.

### WATCHING THE U.S. MARKET

Looking at the growth and trends in the U.S. market, see figure 6, can provide insight into how and why the market has developed there and teach us about the future of the European market.

It is clear that regulation has played a key role in the growth of the U.S. market. Forty-seven states have adopted data breach regulations imposing notification to individuals in case of breach of personal information. With such regulation in place, a data breach costs money because of customer notification and possible penalties in case of regulatory breach. A company with 50 million customers is faced with a potentially significant cost. It is when companies anticipate such costs that they turn to insurance, which is how the market for cyber insurance developed in the U.S. Furthermore, because data breaches must be made public, people become more aware of the risks and, as a result, more interested in buying insurance. This is a virtuous circle.

### State of the market: Key facts



Source: SCOR

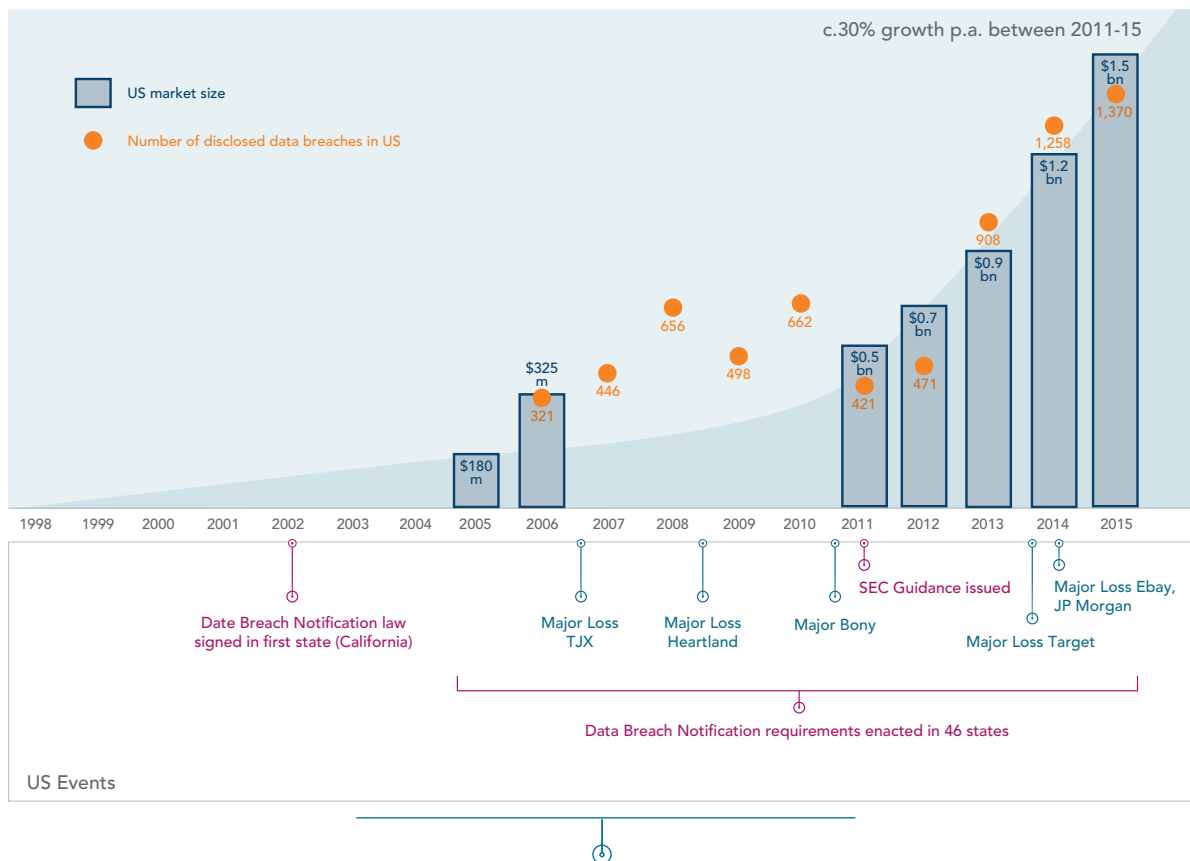


FIGURE 6: HISTORICAL ESTIMATED CYBER MARKET SIZE IN US

Source: AON

The picture is completely different in Europe, which is still a nascent market with approximately USD 100 million in premiums written last year. However, when the GDPR goes into effect, we anticipate that it will stimulate the market in the same way regulation did in the U.S. According to Aon, the European market could write between USD 0.5 and USD 1 billion in premiums by 2020.

## THE REINSURANCE MARKET

Reinsurance is still a nascent market with emerging risks that cannot be priced or modeled adequately. Because reinsurers concentrate the risks ceded to them by insurance companies, the aggregation of cyber exposure coming from cyber

specific or standard products is exacerbated. Developing modelling capabilities to get a grip on clash of risks and cyber catastrophes is a condition for the reinsurance market to grow.

The global reinsurance market is estimated to be worth approximately USD 525M. Most reinsurers have only just entered the cyber insurance market. Because of the modelling and pricing issues mentioned above, it remains mostly a proportional market with approximately 95% of reinsurance premiums being written by reinsurers on a quota share basis.

## CONCLUSION

The cyber threat landscape is undergoing tremendous changes in nature, frequency of attacks, and magnitude of risks. The insurance client base is expanding, with demand evolving from “data breach” coverage to more comprehensive first- and third-party coverage. Incursion of

IT into the “real world” increases exposure to physical loss, blurring the lines between cyber and standard coverage. While the market outlook is promising, the (re)insurance industry requires greater IT expertise to really understand cyber risks and overcome hurdles to market development.



## Summary of the panel discussion on CYBER RISKS AND INSURANCE FOR CORPORATES: A TRUE GLOBAL RISK MANAGEMENT APPROACH AND A NEED FOR FURTHER DIALOGUE

Frédéric Dhers, SBS Chief Underwriting Officer Americas, SCOR Global P&C, moderated the panel discussion on the “cyber risks and insurance for corporates: a true global risk management approach and a need for further dialogue”

The participating speakers were:

- ♦ Philippe Cotelte, Airbus Defence and Space, Head of Insurance and Risk Management
- ♦ Tom Allen, The Channel Syndicate, Head of Technology and Cyber Insurance
- ♦ Steven M. McElhiney, EWI Re, Inc., President



---

### DIALOG AND COLLABORATION

The role of the Risk Manager is to conduct comprehensive risk analysis in order to identify exposure throughout a company. Philippe Cotelte states that this approach requires drawing on the expertise of IT specialists when examining operational risks. The Risk Manager’s primary challenge is establishing credibility by changing stakeholders’ perceptions of cyber risk as an exclusively IT issue. It is difficult to define catastrophic scenarios that encompass a wide range of phenomena, and to determine the functions impacted at each phase, as well as the cost, unless all stakeholders can be convinced to collaborate.

Steven McElhiney states that at NL Industries, a conglomerate made up of disparate business units with unique exposure risks, scenario planning is viewed as an enterprise function. The company’s efforts are complicated by the fact that 90% of the knowledge necessary to combat cyberattacks resides within IT. Because of this asymmetry, it is essential to collaborate with IT in order to be effective.

On a broader scale, Steve McElhiney points out that despite the strong alignment of interest among the insurance industry, government and other parties, he finds there is insufficient collaboration when it comes to finding solutions. He believes this is not only a major challenge for the insurance industry, but an industry crisis at national and international levels.

However, there is progress in this area. Philippe Cotelte describes a yearlong collaborative research project that included Airbus, the French national information systems security association (ANSI), and the public research laboratory, Systemics. The project also involved the OECD, the French government, the French insurance federation, French and European risk management associations, brokers, lawyers, and actuaries, among others. The group published a report containing new industry recommendations that will likely be promoted at the national, European and OECD levels.



Recommendations from the cyber risk research report published by SystemX-IRT

- 1- Promote Quantified Risk Analysis managed by the risk managers
- 2- Promote a common language and reference on cyber risks with insurers
- 3- Improve communication and clarification on insurance coverage of cyber risks
- 4- Build the conditions of a trusted dialog between insured and insurers
- 5- Provide more certainty on legal definition of cyber risks

## SCENARIO PLANNING

According to Philippe Cotelle, companies must attempt to identify the evolution of exposure in terms of cost and time. The Airbus methodology to devise catastrophic scenarios identifies not only specific targets, but also the different business functions that could be impacted. Part of the process includes defining attackers' profiles, motivations, and what kind of organizations they belong to. The final element is estimating recovery time in collaboration with operations. Airbus breaks down each scenario into three phases: the crisis phase (when an attack is discovered), the remediation phase, and the vigilance phase. The results of the company's studies show that the most costly phases in a catastrophic scenario are remediation and vigilance resulting from loss of business efficiency due to mitigation actions. Risk Managers need information such as this when attempting to evaluate mitigation costs.

Unlike 40% of U.S. companies, NL Industries does not have cyber insurance because it does not address the specific needs of a B2C company that stores relatively little personal user data. However, contingent business interruption is a major risk exposure. Steve McElhiney argues that it is important to have predefined disaster response plans for cyber and real-world incidents. The company spends a great deal of time on scenario assessments, planning how it would mitigate its exposures, and real-world testing, including first-responder drills (for Property & Casualty) and bringing in covert IT experts to test the company's cyber defenses.

“OUR BIGGEST RISK IS COMPLACENCY; BELIEVING FOR SOME REASON THAT WE ARE NOT AS EXPOSED AS OTHERS.”  
*Steven M. McElhiney*

## RISK TRANSFER

Philippe Cotelle supports the view that before arriving at a point where risk is transferable, companies must reduce the likelihood and cost of the risk. Once it has been mitigated for the most part, it can be treated like a regular risk with the potential to be transferred. Investment in IT is required to reduce the probability of occurrence. When these costs become too high, insurance becomes complementary (and not competitive) to IT measures and is efficient from a costs point of view.

Companies need to demonstrate that a risk transfer has value. However, before insurers can see the value in a risk transfer, they would require access to sensitive information, which companies may be reluctant to disclose. As a result, insurers may only have access to limited and inadequate information.

Claims directly affect the potential for risk transfer: the effectiveness of insurance is limited if companies are unable or unwilling to settle claims. Although a company may choose not to make a breach public, or even publicize it internally, to file a claim it must nonetheless inform its insurers. Experts may be called in to evaluate the extent and value of the claim. As a result, information that could harm the company's reputation is revealed to outsiders. Companies may choose not to file a claim for an attack rather than risk the consequences of this knowledge getting out.

## MARKET LOSSES

Tom Allen states that the most volatile elements in losses to date are the investigation phase, liability and indemnity. The investigation phase requires engaging a forensic investigation firm, which is expensive and can entail months of work. This is necessary in order to establish proof of loss and is also a basis for liability. Underwriters anticipate notification costs, but often overlook liability as a significant loss factor. There are currently loss adjustment regimes in place, or significant penalties (up to 2% of global turnover) in the U.S. and the E.U.

He adds that business interruption claims are more rare than others in the cyber context, partly because of the relative unpopularity of the coverage over time, or the evolution of and experimentation with triggers. Business interruption coverage is a challenge for underwriters because the policy language is not particularly clear, loss adjustment protocols are not agreed on in advance, and there are few precedents to rely on. This presents a major challenge that will require insurers to move beyond their comfort zone.

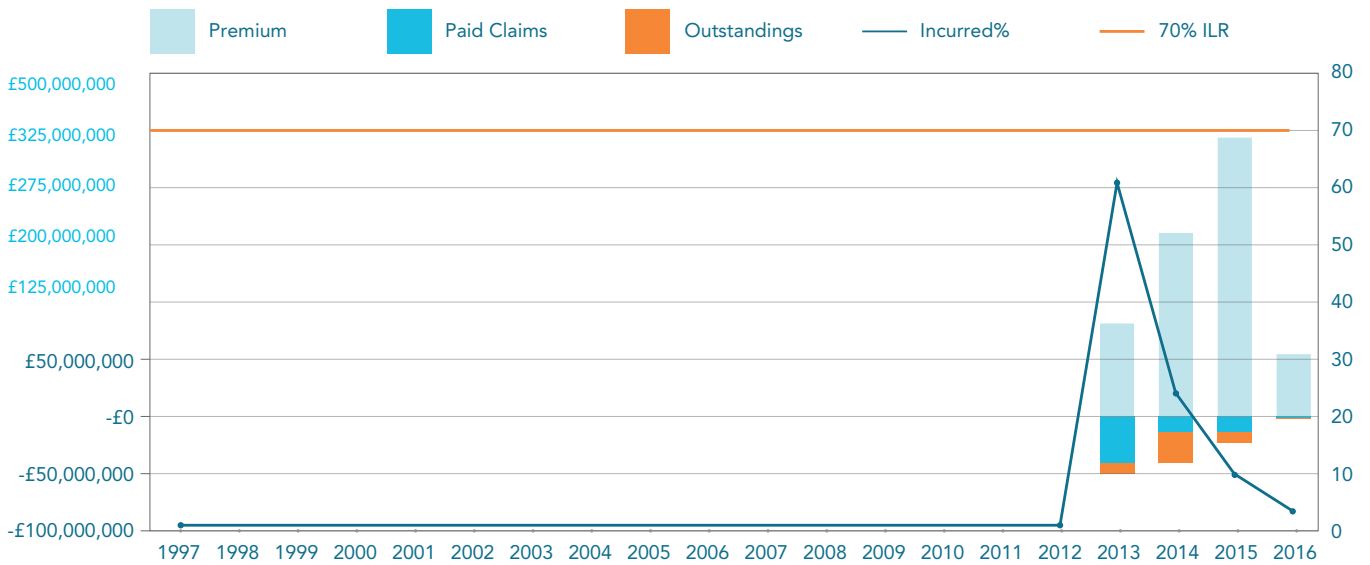


FIGURE 1: ACTIVITY, CHANGES IN LEGISLATION, THE DEVELOPMENT OF THE BREACH MARKET, AND LOSS DEVELOPMENT

Source: LLOYD'S CY RISK CODE SUMMARY Q2/2016.<sup>1</sup>

## LOSS ADJUSTMENT AND UNDERWRITING CHALLENGES

Tom Allen states that it is important, particularly in the case of claims made on the eve of policy renewal, to precisely define which factual events trigger coverage. Current policy language is inconsistent, and most policies are on a claims-made basis, which increases the potential for mixed triggers (a claim could be filed when a loss is discovered, or when a system is compromised).

The industry needs to be able to more accurately value loss. Forensic investigation commissioned by or on behalf of the insured is meant to establish the cause and extent of a breach, but it does not address the financial impact on the insured.

The way clauses are applied also needs to be examined. A policy with primary coverage that has a war and terrorism exclusion with a buyback clause for cyberterrorism could include excess coverage that does not. This can result in disputes over payment of claims. Further, the utility of such clauses is limited due to difficulties with attribution.

There is discontinuity between primary and excess markets. There is no loss adjuster appointed on behalf of the market, which results in the primary insurer acting in its own best interest to the detriment of the underwriters of the excess coverage.

“WE WOULD BE ABLE TO DEVELOP MUCH SHARPER PRICING MODELS AND A MUCH GREATER APPETITE AND CAPACITY FOR RISKS IF WE HAD MORE OF A SENSE FROM THE INSURED ABOUT WHAT THE RISK LOOKS LIKE TO THEM AND WHAT THEY REALLY NEED.” *Tom Allen*

1 - There is likely a three-year tail on data breach claims, and this table represents only breaches that syndicates have been reported to Lloyd's





With regard to underwriting, underwriters need to understand an insured's business model, as well as a high level of sector knowledge in order to conceptualize risk. Pricing risk requires subjective disclosures about the risk characteristics of the insured as well as exposure data. Risk control information is needed to assess whether a risk is good or bad. Finally, underwriters need a sense of the loss context to undertake the risk.

Pricing models should be based on a close examination of the risk that needs to be underwritten and validation of the risk to the extent possible using available data. Conceptually, there is no barrier to developing pricing models around first-party dependencies and values, but most of the market is still using professional liability rates. If the industry does not have robust pricing models in place now, it will not be ready when it needs to transfer the pricing of cyber exposures into the automobile market, for example.

---

## CONCLUSION

Philippe Cotelle does not believe it is insurers who will drive companies to be more cyber secure. Rather, he believes that regulation, as well as pressure from investors for more transparency with regard to cyber risk management is what will motivate companies to improve. Neither does he believe we have reached the point where companies see the value in cyber insurance. This should change as risk managers and insurers catch up to technology, and cyber risk management becomes increasingly valuable to companies.

Steve McElhiney takes the view that carriers need to come up with more customized solutions, as in the past. He adds that NL industries does not lend itself to modelling due to unique exposures that need to be underwritten individually.

---

"REGULATION, AS WELL AS PRESSURE FROM INVESTORS FOR MORE TRANSPARENCY WITH REGARD TO CYBER RISK MANAGEMENT IS WHAT WILL MOTIVATE COMPANIES TO IMPROVE."

*Philippe Cotelle*

---

In fact, the company is exploring the possibility of using its captive insurance to create a policy tailored to its needs, as well as facultative reinsurance to reduce the severity or the costs. He believes that customized coverage is a challenge, and it presents nascent market opportunity for carriers. He adds that insurers can offer companies tremendous value by having claims processes for indemnity, as well as remediation in place and ready to use.

Tom Allen states that cyber insurance currently attempts to offer many features at a competitive price, making it unsuitable for specific industries. He believes that the way forward as underwriters is to evolve towards industry-specific product offerings.



# TECHNOLOGY: SHAPING THE RISK LANDSCAPE

## Victor Peignet, CEO, SCOR Global P&C



**VICTOR PEIGNET**  
CEO  
SCOR Global P&C



**Victor Peignet has been the Chief Executive Officer of SCOR Global P&C since 2005. He joined SCOR in 1984 as an underwriter in the Technical Risks Department.**

He then successively held the posts of Manager of the Offshore & Marine Department and Manager of the Marine & Energy Sector. He served as Deputy Managing Director and Managing Director of SCOR's large corporate accounts division (SCOR Business Solutions) from January 2000. Mr. Peignet is a marine & offshore engineer who graduated from the Ecole Nationale Supérieure des Techniques Avancées (ENSTA).

## TECHNOLOGY IS CHANGING THE GLOBAL RISK LANDSCAPE

Technology is a broader topic than cyber, but the two are, closely related. Technological advances continue to reshape risks around the world. We can choose to consider these changes either to be daunting threats for which we have no solutions... or new opportunities. After all, risk is what we are here for as insurers and reinsurers. We should welcome the opportunity to help customers protect themselves.

Of course, we have no control over the timing of the opportunity, which is less than ideal. It is much easier for companies to invest in innovation and take new risks when margins are ample. Insurers and reinsurers are in an environment where interest rates are very low, where our industry is highly competitive, and where there is too much capital. This means that we have to approach new risk with a long-term view, to measure what it represents, and to ensure that the choices we make are consistent with our duty to deliver profits to shareholders while meeting requirements from stakeholders.

### RISK PREVENTION HAS GREATLY REDUCED LOSS FREQUENCY IN TRADITIONAL RISK CLASSES

Risk management introduced, provided, or encouraged by insurers has worked: measures of traditional losses are down greatly over the long term, as shown in Figure 1. We take risks through a domestication process, like taming a species

of wild animal. Insurers should take pride in the extent to which we have contributed to such improvements by introducing risk management, loss control, risk prevention, and domestication of risk.

The (re)insurer's mission is to take a risk and find ways to mitigate, control, or eliminate it, working with insureds, government bodies, and other stakeholders. Over time, risks become commoditized and margins fall. This is why the insurance industry cannot exclude its way to greatness.

The industry is reaching a point where business must be regenerated by taking on new risks. In the current climate, insurance companies that have the necessary knowledge, the means to invest, and the ability to restart a process of domestication will have a competitive advantage.



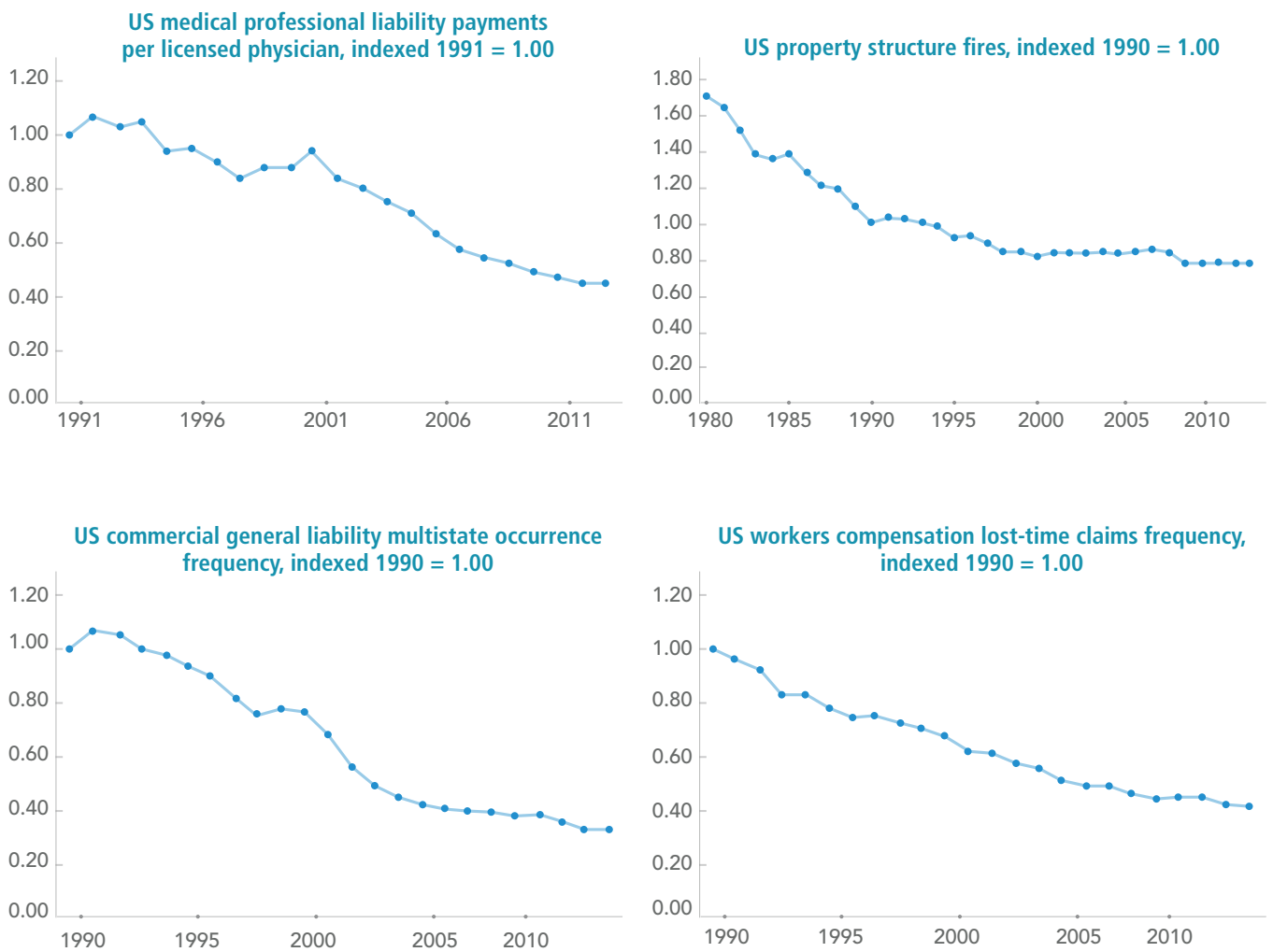


FIGURE 1: REDUCTION OF LOSS FREQUENCY BY THE (RE)INSURANCE INDUSTRY IN TRADITIONAL RISK CLASSES

Source: Aon Insurance Risk Study 2015

## CONNECTIVITY AND SYSTEMIC RISK

Risks are increasingly systemic because of the high degree of connectivity worldwide (see figure 2). Further, the fact that the same technology standards are used globally in all industries results in shared dependencies on certain providers, which also increases risk.

The blurring of the boundaries of time and space – it is easy to cross borders online – changes risk accumulation and aggregation patterns, which is becoming a real challenge to the (re)insurance industry. In certain cases, we are facing the

problem of accumulation propagation. However, if we draw up scenarios that are too catastrophic, we are incapable of moving forward. It is important to improve our approach to finding realistic estimates of maximum possible loss. With better modelling and estimates, risk can be addressed.

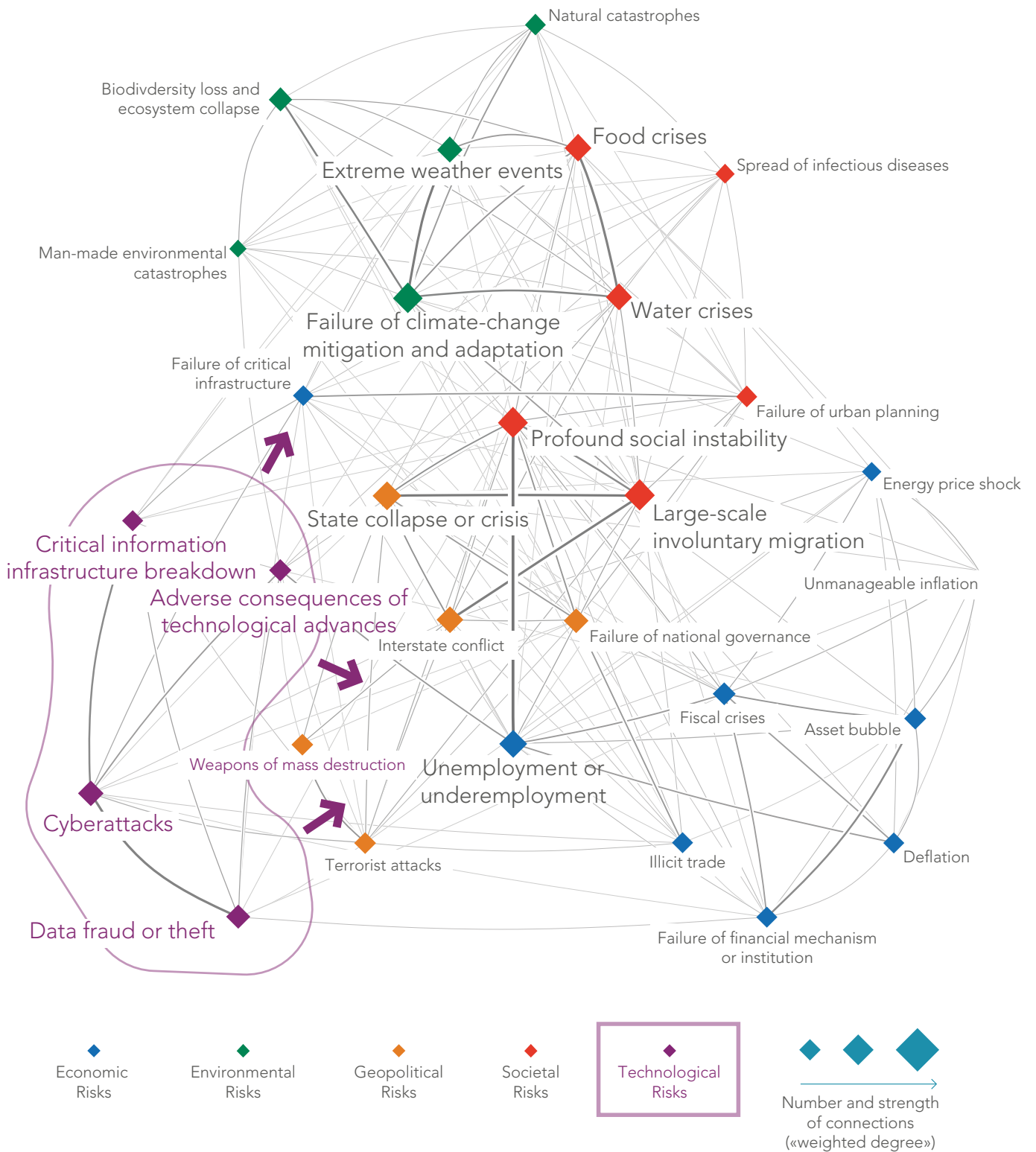


FIGURE 2: WORLD ECONOMIC FORUM RISK MAP (TECH IN PURPLE)

Source: Global Risk Report 2016 - WEF



## CHALLENGES TO DOMESTICATING CYBER RISK

Intangible assets are largely unaddressed by current market products. Every company has them. What is new is how large they have become (see figure 3). Historically, we have had no solution for protecting such assets, but they were smaller and companies accepted them as an enterprise risk with basically no coverage. Today, however, with many companies recognizing that their value depends primarily on intangible assets, they are increasingly eager to find solutions to protect them.

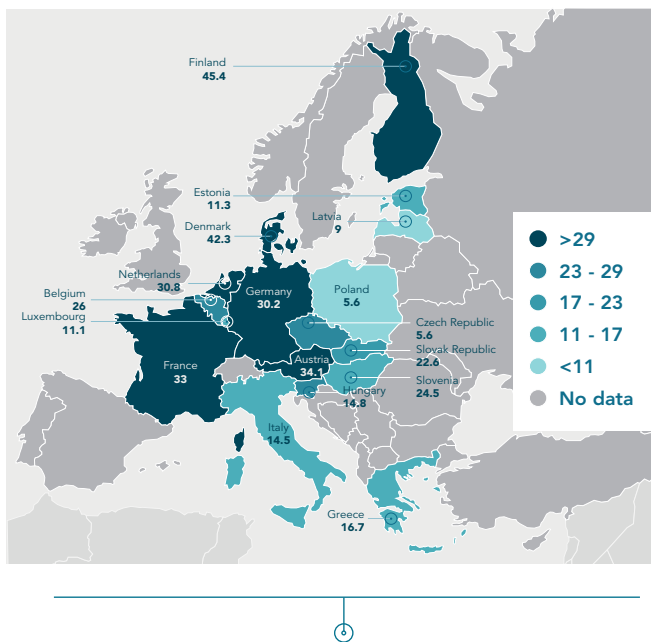


FIGURE 3: INVESTMENTS IN INTANGIBLE ASSETS IN % OF GDP

Source: OECD, 2015

For example, at SCOR, we run our entire business on a proprietary computer system, which is a significant competitive advantage. How do we determine the value of that system, and how do we protect it? If that system failed for any reason, how would we run our company?

Historically, insurers have had a degree of control over the claims: loss adjusters and experts discuss with the insured what will and will not be covered by the insurance. In the cyber context, however, companies must react immediately. There is no time for discussion and no time to send experts. Clients take steps to rectify the situation and insurers pay the bill.

Pre-underwriting investigations to analyze the cyber risk of large corporation could represent a sizeable sum. So it is important to overcome this kind of obstacles, yet with certain products and risks the obstacles are so enormous that they can prevent the solutions from emerging at all.

“IT WOULD BE BETTER TO HAVE EXPLICIT CYBER COVERAGE THAN IMPLICIT. OUR CHALLENGE IS IDENTIFYING WHETHER TO OFFER CYBER INCLUSIONS ON EXISTING POLICIES OR PURE CYBER PRODUCTS.”

Furthermore, underwriters today continue to calculate rates and pricing as multiples of the property rate, which is inadequate: they need to think in terms of exponential values.

Because cyber risk is a new risk, we have silent exposures in our policies, where cyber losses can come from even if cyber is not mentioned in the policy.

Even when coverage is explicit, it is difficult for the (re)insurers to assess direct and contingent exposure to major events, such as the Thai floods (2011), the Tianjin explosions (2015) and Hurricane Andrew (1992). With Andrew, a record-setting hurricane, the market was caught completely off guard. Years later, when Katrina occurred, the insurance industry reacted, but was more prepared. Though we still have much to learn, experience teaches us that we cannot avoid losses, we can just avoid being caught by surprise by them.

Current catastrophe or aggregation models only address physical events with geographical limits. This offers an opportunity to revise our approach to modelling. There are surely losses we are not expecting and chains of causation we have not anticipated that could be of such a magnitude that the market will be unprepared. Our emerging risk specialists are working on scenarios, but we cannot anticipate every situation.

But we must improve because clients want solutions covering the total risk, encompassing security (breach, failure or wrongful act) and system failure related causations with claims made type provisions and sub-limits.

Beyond existing cyber, we also have to consider the Internet of Things – autonomous cars, wearable devices, industrial controls, etc. This trend, while still in its infancy, will create product risks and shift liability to a degree that we are not yet able to quantify.

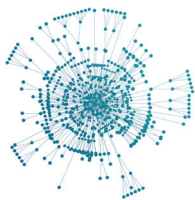


# TECHNOLOGY MAY BRING SOLUTIONS

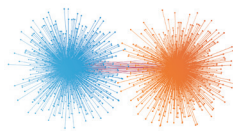
## SOLUTIONS FOR EMERGING RISK: SUPPLY CHAIN

Developing predictive models based on real-time analysis of industrial connections could improve our assessment of business disruption. In the image below, you can see the similarities between supply chains and an IT network. At the pre-loss stage, the analysis of Internet traffic could provide insight into client-supplier business relationships, enabling us to identify a concentration of nodes representing critical suppliers to an entire industry, for example. The volume of data exchanged between a supplier and its customers could also indicate the size of the business.

Supply Chain



IT network



Another source of insight is to aggregate data from dynamically tracking goods in transit from the supplier to their final destination by means of Radio-Frequency Identification (RFID) devices. By tracing goods, we can improve our knowledge of the supply chain, possibly identifying exposure before loss occurs. This would also allow us to compute the value of assets or stock in a given location in real time.

We could take similar post-loss measures. For example, if we see that the IT traffic in an industry or large manufacturer has suddenly slowed or stopped, it could indicate a business disruption, which is an argument for tracking specific data flows. Although it would not prevent loss, this approach could provide information regarding the size of a loss, or an early warning of the seriousness of an incident.

## SOLUTIONS FOR EMERGING RISK: BUSINESS DISRUPTION AND ACCUMULATION

We can draw a parallel between mapping the connections in a supply chain and mapping connected industrial systems. Industrial systems already collect information on their clients' devices for purposes of maintenance and usage data. Aircraft manufacturers, for example, have optimized maintenance operations by deploying real-time information exchanges. Again, this should provide some information

about common vulnerabilities. If a number of customers are connected to the same supplier, then they have purchased the same services, or bought the same goods. To get an idea of the extent of the accumulation of system risk, one approach could be to leverage these maps of connections.

When we work with insurers on casualty issues and catastrophic casualty exposure, we have to admit there are many risks of which we are unaware. A few years ago, we launched a research project with some partners to test the use of data as an early risk warning system. The objective is to collect data and determine at what point we should become concerned about a risk.

Take, for example, a new chemical compound that becomes available and is simultaneously integrated into a variety of products in different industries. If we could monitor scientific publications that reference the compound and liability lawsuits related to it (particularly in the U.S.), we might be alerted to potential problems and be able to decide whether the compound is something we want to cover, or adjust the price of our coverage to send a signal about risk. This is similar to existing efforts to predict probabilities of widely used chemicals to cause casualty losses and mapping their use throughout industry.

## SOLUTIONS FOR EMERGING RISK: LINK BETWEEN CYBER AND WAR/TERROR

For insurers and reinsurers covering war, terror and political risk, monitoring data flows can also be useful in detecting, assessing and modelling political risks and the imminence of problems. Cyberattacks have been linked to warfare and aggression as in the cases of Russia and Georgia (2008), North Korea and the Sony hack. In addition, terrorists use social networks extensively for propaganda and recruitment.

## MODERNIZING INSURANCE CULTURE

Everything I have discussed so far requires a change in the (re)insurance industry culture towards multi-dimensional, cross-class approaches. In the context of cyber risk, for example, underwriters need skills to analyze each and every aspect of a particular risk. They must not work in silos of their lines of business, but work in a project team with a multi-disciplinary project manager.

Underwriters not only need to converge and share the relationship with the client, but they also need to converge on one view of risk, drawing on all of the different disciplines in the company.



Our industry needs to develop or attract people, and who can bridge the communication gap among the generations: people who understand the “new new” generation, the “new” generation and the “old” generation with its highly valuable experience.

The ability to perform predictive analysis is more important today than experience rating, which challenges actuaries to think differently. Still, they need data. In order for insurers to perform risk assessment on a company in a technology or cyber context, clients need to be willing to reveal secrets to insurance companies. In a subscription market scenario, a company being assessed could potentially need to provide access to sensitive information to multiple insurance companies. Another concern is the relationships and division of responsibilities of the co-insurers in this context.

Because cyber risk is immature and changing daily, we need to be careful about offering insurers a binding, one-year agreement without being allowed to review the risk assessment during the course of the year – moving towards a metered approach rather than a flat rate.



Cyber risk is evolving so fast that it is surprising the market is willing to cover it without clauses – similar to those we include in political risk and terrorism policies – that allow insurers to reconsider the conditions if something new occurs to change the forecast.

## SCOR: NAVIGATING CHANGES IN THE RISK ENVIRONMENT

At SCOR, we have been working for almost two years on performing risk mapping and assessment and making comparative risk assessments by industry sectors. The logic behind this approach is that different industries do not have the same exposure to the same risk, and it is best to target our approach to each client’s specific commercial and technical needs.

Our current challenge is developing the expertise, models and tools we need to properly address the issues of risk selection, pricing and accumulation. Accumulation is a major challenge at the moment. As for risk selection, we need to understand clients’ business and its value chain in order to be able to discern what is essential to them, which will allow us to focus on covering critical risk only. To do this, we need to perform mapping by industry sectors.

Without reliable pricing or accumulation tools, we do not know how to price cyber coverage. Yet we must start somewhere. Therefore, it is advisable to be selective and make decisions about what to cover based on the situation at the time.

In addition to cyber, we have many new projects involving data, the amount of which has increased significantly in the last five years. We have done considerable work in the area of Property and Casualty (P&C) in agriculture and natural catastrophe, for example. We have made significant

progress in Life because we have had more data available – and for a longer time – for Life than P&C.

Even before the recent surge in interest in InsurTech, SCOR has partnered with numerous data, analytics, and technology-driven companies, both start-ups and established firms, to augment our capabilities. Additionally we have supported industry-wide efforts to combine resources towards common goals. We are encouraged by start-ups reimagining insurance products and services to close the protection gap, such as by developing cyber protection and insurance in a combined offering that may be more attractive to some buyers than individual products. Many start-ups will generate valuable research & development that will ultimately be beneficial to the insurers and reinsurers who take advantage of it. We are encouraged by start-ups reimagining insurance products and services to close the protection gap, such as by developing cyber protection and insurance in a combined offering that may be more attractive to some buyers than individual products. Many start-ups will generate valuable research & development that will ultimately be beneficial to the insurers and reinsurers who take advantage of it.

As mentioned above, the insurance industry can be regenerated by taking on new risks. Consider figure 4, which depicts the risk lifecycle. The lifecycle starts with nascent risk, at which point you are aware of a risk but are unable to quantify it. At this stage, there is no risk transfer.

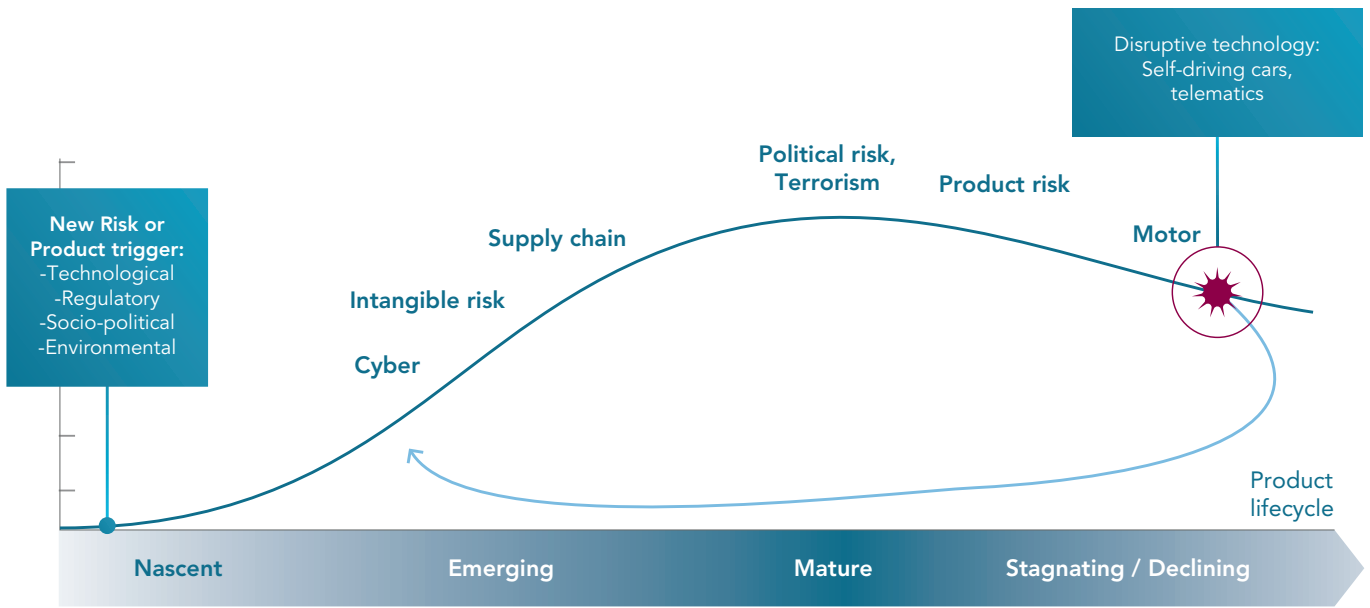


FIGURE 4: MANAGING BUSINESSES ALONG THE RISK AND PRODUCT LIFECYCLE

Source: SCOR

When a risk is emerging, transfer becomes possible, although it is still inadequate. This is where cyber risks and intangible assets are at present. The market has mishandled the supply chain in this context, but now there will be another opportunity to take it into account

Finally, once a product is mature, it reaches the commoditization stage. This is when reinsurance becomes irrelevant. While some products will decline, practically disappear, and be commoditized, others will rebound because some

catalyst in society, the environment, or technology will radically change the risk and exposure, thus restarting the cycle. For example, autonomous cars may soon regenerate automobile insurance, albeit potentially with much lower premium volume than before.

Insurance is a business of constantly reinventing products and domesticating new risks. Insurers and reinsurers that do this well create the best long-term value.

## CONCLUSION

The (re)insurance industry is going through a difficult transition in which we do not have adequate profitability to invest in new risk. We should be optimistic. The industry has tackled many new risks in the past, so we can tackle at least some of these new risks, as well as the traditional risks that are regenerating. Our challenges are to obtain the right resources, adapt our culture, and offer reliable solutions that, at the same time, appeal to our customers and are viable for us over the long term.







# Summary of the panel discussion on MODELLING AND PRICING CHALLENGES

**Simon Dejung, Engineering Underwriter, SCOR Global P&C, moderated the panel discussion on “Modelling and pricing challenges”.**

The participating speakers were:

- ♦ Serge Droz, Open Systems, Vice President OS-CERT
- ♦ Jean Donio, University of Paris II, Professor Emeritus
- ♦ Roger Iles, Nanyang Business School, NTU, Insurance Risk and Finance Research Centre Senior Research Fellows

Jean Donio opened the discussion by suggesting that attitudes and approaches within the insurance industry need to change in order to prepare for the future. He also noted that, although the role of insurance is traditionally thought to be to respond to random events, the industry

must be aware that, in fact, it warrants the economies of the entire world. Lastly, he pointed out that factors that are usually ignored, such as significant cultural differences among countries.



## EXTRACTING VALUE FROM THE DATA

To guide the discussion, Simon Dejung drew on excerpts from the report “Examining the Costs and Causes of cyber Incidents” written by Sasha Romanosky and based on a study by the RAND Corporation. This study, which used Advisen data for 12,000 cyber incidents, found that the median loss over the sample was less than USD 200K. This suggests that less than 1% of a company’s annual revenues are likely to be at risk in the event of a cyber incident. For purposes of this study, incidents of different types were grouped together, an approach that could help in defining different types of cyber coverage and insurance products.

Roger Iles agrees that incident data must be grouped in order to obtain reasonable statistics given the paucity of available data, but emphasizes the importance of understanding the risks associated with different incidents, and of grouping incidents in terms of like risks. With regard to the RAND report, for example, he questions whether grouping Intellectual Property (IP) losses with those resulting from Distributed Denial of Service (DDoS) attacks

is an appropriate collection of risks, given the different motivations of the attackers.

He agrees with Dejung that standardized labeling of data proposed by the CRO forum might be a better approach<sup>1</sup>.

He emphasizes that data must always be examined for biases and limitations, and suggests that, due to underreporting, the Advisen data set likely lacks data on smaller events. However, such events may not be relevant to the insurance industry since, as Dejung points out, they would be covered by deductibles.

Iles continues, stating that regulation and the statutory reporting of events are key if insurers are going to collect a data set, which is essential in understanding risk. In the U.S., the Securities and Exchange Commission filings provide information about potential losses. Reporting will be coming to Europe<sup>2</sup> - but is not required in Asia at present. However, Singapore may institute reporting next year.

1 - <http://www.thecroforum.org/concept-proposal-categorisation-methodology-for-cyber-risk/>

2 - [https://en.wikipedia.org/wiki/General\\_Data\\_Protection\\_Regulation](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation)

<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>



## PUTTING THE RISK PROFILE TO WORK

Iles states that underwriters need to consider an organization's risk profile, which goes beyond its levels of IT security. It also involves understanding its attractiveness to hackers, and specifically to which type of hackers. The nature of a business strongly influences its attractiveness as a target, and the type and probability of attack. It is also essential to understand the motivations of attackers and the kind of exposure this entails. Understanding this provides insight into the types of losses an attack might generate.

Serge Droz supports the view that it may not be valuable in the insurance context to understand how an attack occurred. He suggests that, rather than focusing on technical details,

the industry should focus on the financial effects. He cites the example of health insurance, which is calculated not on the health of individuals, but on statistics.

Dejung notes that underwriters are already taking these factors into account, offering, for example, sublimited coverage for industries that might be liability prone or at risk of a major business interruption.

## GETTING PAST PERCEPTIONS

Dejung observes that there seems to be some reluctance to provide cyber insurance to the financial industry. The RAND study does indeed show that the total number of cyber incidents is the highest in this industry, but it also shows that

this industry does not have the highest incident rate. This indicates that the likelihood that cyber insurance for the financial industry – or others with high total incidents – will be affected is not as great as might be perceived.

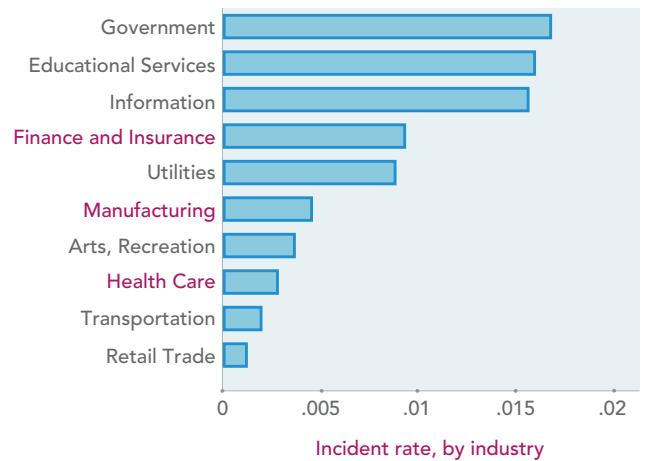


FIGURE 1: CYBER INCIDENTS AND RATES BY INDUSTRY

Source: RAND

Further, the study shows that, in terms of total costs of loss from cyber incidents, finance/insurance ranks fourth.



Again, the order changes when these industries are ranked by cost of loss per event, with finance/insurance falling to seventh place.

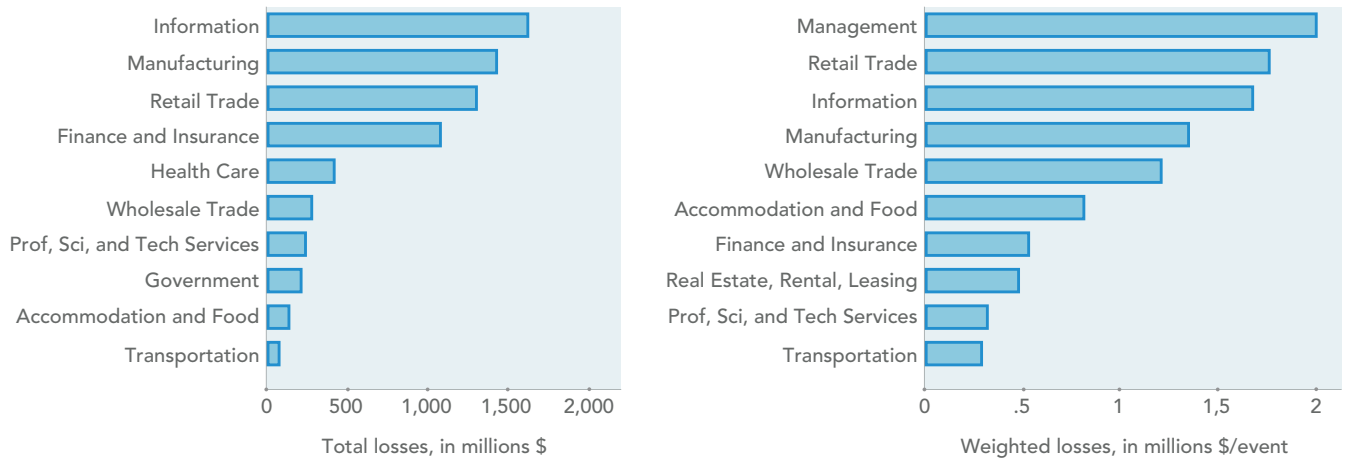


FIGURE 2: LOSSES BY INDUSTRY

Source: RAND

Droz interprets these differences to be a reflection of the cyber maturity of the different industries, finance likely being the most mature because, as a high-profile target, it has had to implement robust cybersecurity. He emphasizes that perceptions of risk must be addressed and taken into account in performing risk calculations.

Iles adds that perceptions with regard to cyber risk are strongly influenced by the press. He points out that the median loss of USD 200K from the RAND study is substantially lower than losses typically reported by the press, which tend to report average or mean figures in the USD 1 million - USD 2M range. Only major events are reported in the press.

To provide perspective, the RAND study also compares traditional losses as a percentage of revenues, such as shrinkage, bad debt and fraud to those caused by cyber events:

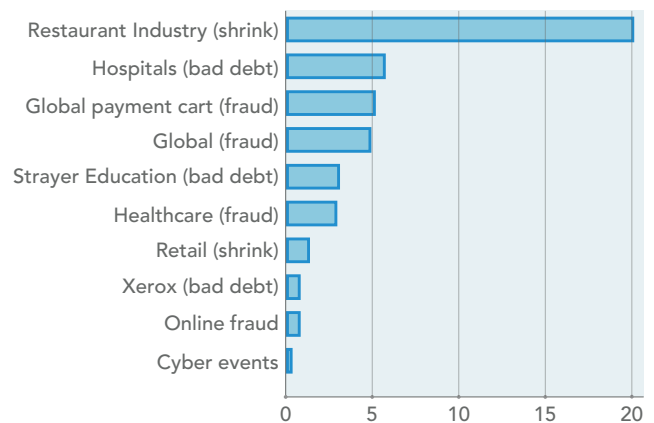


FIGURE 3: LOSS AS A PERCENTAGE OF REVENUES

Source: RAND



Iles believes that the relatively low ranking of cyber events in this comparison may confirm that most events are relatively small. This, plus the fact that major attacks require significant time, effort and expertise, may support the argument that major events are less likely to occur.

He agrees with Dejung that, in this case, mass insurance products, and risk-sharing models might be a viable pricing approach for more standard cyber losses, such as data breaches, but emphasizes that the cyber landscape is still changing. In the case of larger contracts, like industrial companies, he proposes a more facultative approach, stressing that without a deep, hands-on understanding of the vulnerabilities of such companies an insurer would not be in a position to underwrite the risks.

He goes on to point out that systemic risk, resulting in traditional losses, is the real danger, and that the major events we have seen have not been accumulation events. Accumulation leads to losses in multiple areas and can trigger non-cyber coverage. He suggests that cyber insurance could resemble traditional property insurance, with basic policies to cover attritional and some large losses, and catastrophe policies to cover systemic events.

The RAND study also shows that losses from cyber events and cybercrime are relatively low compared to the average for all types of losses:

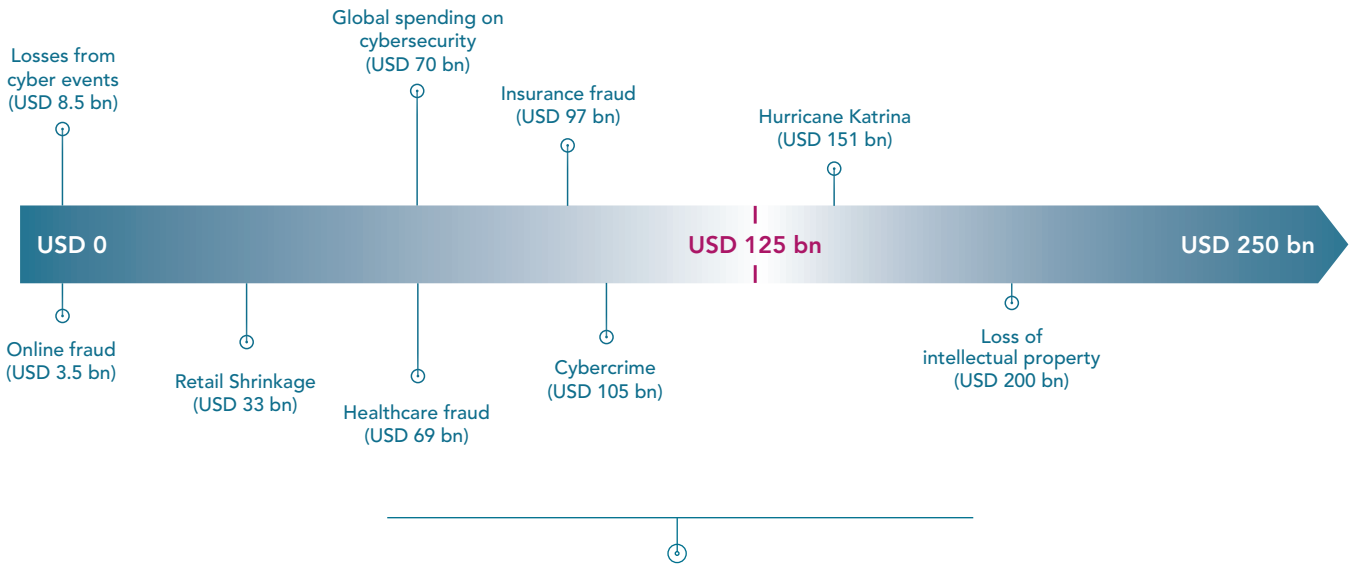


FIGURE 4: RELATIVE COSTS AND LOSSES OF CYBER INCIDENTS

Source: RAND

Iles states that losses from cybercrime are probably higher than from other types of cyber events due to litigation costs. He suggests that this could change, adding that we must keep in mind that cybercrime is increasing, and that attackers' methods, the complexity of attacks, and the sophistication of technologies are changing rapidly. In the last year, ransomware attacks have significantly increased, litigation is changing rapidly, and U.S. legislation is coming into play in Europe. The nature of losses can change with such conditions, which can differ drastically from one year to the next. These factors must be considered when modelling risk and losses.

Droz states that, although cyber incidents are increasing significantly in absolute terms, relatively speaking, the general cyber context could be considered to be improving

because of the exceptional benefits and potential IT offers society. He does not believe cybercrime-based risk is as high as people perceive it to be, although agrees that we must remain vigilant. He makes the distinction between supposed and actual damages, taking the example of the music industry, which continually claims losses in the billions – a fictitious number – due to illegal downloading. Stealing copyrighted material results in much less actual loss than is usually reported. This is a key point to keep in mind in the insurance context.



---

## PROACTIVE APPROACHES TO INCREASE CYBERSECURITY AND REDUCE RISK

The RAND study shows that the majority of companies experience cyber incidents only once. Dejung suggests that underwriters take repeat attacks into consideration and that, in response to failure on the part of companies to implement better cybersecurity, the industry might establish prerequisites without which insurers could reduce or refuse claim payments.

Droz agrees that insurers should require evidence of a certain level of cybersecurity from clients. He adds that it is not necessary for enforcement or auditing to be done by insurers themselves, citing the financial industry, which has rigorous auditing procedures in place. Insurers could accept third-party certification from expert IT auditors who could verify the quality of clients' cybersecurity.

He observes that when companies experience a breach, it generally serves as a wake-up call and motivates them to strengthen security, while others do not seem concerned. The absence of repercussions may be behind this lax attitude. To manage exposure to repeat incidents, insurance companies could institute something similar to a three-strike program in which coverage is cancelled after a certain number of breaches, or some variation on serial loss clauses.

Iles agrees that, without legislation, companies have no incentive to boost their cybersecurity. He also supports the view that it is the role of the insurance industry to drive improvement in cybersecurity, as well as to provide awareness and understanding, particularly for SMEs (Small Medium Enterprise).

To reduce risk, Droz supports the view that a preventive "cyber hygiene" approach, similar to proactive wellness

programs increasingly adopted by the healthcare industry, could be applied in the cyber context. The insurance industry is in a position to create incentives for companies to be more secure by offering lower premiums and insisting on compliance with certain standards. He states that although average companies may never need cyber insurance, they should not discount it. SMEs are particularly vulnerable: a loss of USD 200K can threaten a small company's existence. He suggests that a partial coverage model in which risk is shared may be more appropriate. He believes such a model has considerable potential, and that it should be explored by the IT and insurance industries.

Iles adds that it is very important for insurers to have a realistic awareness of what cyber is. The industry should drive the implementation of cybersecurity, as well as provide awareness and support to companies, particularly SMEs, which may not be able to pay for such services. Moving them to the cloud, for example, could change the risk quite substantially. This could potentially increase systemic risk, but would reduce attritional risk and probably have a significant impact on the economy if it continues to increase. The focus would then have to shift to managing the systemic risk more carefully, an area that requires more research.

Droz states that much more data is needed, and that governments are becoming aware of this. The more cyber insurance is adopted, the more data will be collected because insured companies will have incentive to report incidents. Fears of reputational damage in publicizing breaches may be excessive. He cites the example of Kaspersky, a major antivirus software company: after the announcement of a breach, the company's sales rose because the public responded positively to its transparency.

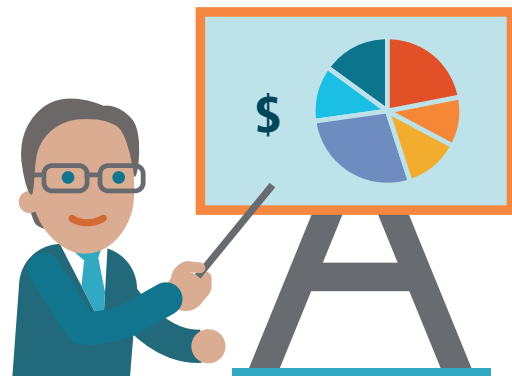


# Summary of the panel discussion on AGGREGATION AND CLASHES MONITORING

**Paul Nunn, Head of Catastrophe Risk Modelling, SCOR Global P&C, moderated the panel discussion on "Aggregation and Clashes Monitoring".**

The participating speakers were:

- ♦ Phil Holt, Senior Catastrophe Risk Analyst, SCOR Global P&C
- ♦ Scott Stransky, Assistant Vice President and Principal Scientist, AIR Worldwide
- ♦ Christos Mitos, Vice President of Model Development, RMS



## MODELLING METHODOLOGIES

In his introduction to the panel discussion on cyber Aggregation, Paul Nunn agreed with earlier speakers that reinsurance has a key role to play in supporting the development of the cyber insurance market, and the potential for cyber premium growth to ~USD 9bn by 2020 was surely an opportunity for our industry. A key challenge for both insurers and reinsurers, however, is the need to develop a framework to underpin articulation of a cyber Risk Appetite and the means to monitor cyber coverage sold against a cyber Risk Tolerance. To date we have seen some notable individual insured cyber losses, but in an increasingly interconnected world, we can see concentrations exist that could lead to claims from multiple policyholders simultaneously – a cyber catastrophe. Much of the early work in developing deterministic and probabilistic approaches to understanding such risk aggregation has been done by catastrophe risk modelling firms, and also in the Lloyd's market, and this panel brings together experts from these areas to discuss new developments and challenges in managing cyber risk aggregation.

Scott Stransky and AIR support the view that a cyber incident on a par with Hurricane Andrew is somewhat likely to occur in the next few years. If the cloud were to go down, for example, it could cause multiple, simultaneous business interruption claims resulting in billions of dollars in losses for many insurers across the board.

In terms of deterministic cyber risk modelling, the AIR methodology takes a detailed accumulation approach as opposed to a purely market share-based approach. Rather than analyzing risk based on a percentage of companies that use a particular cloud service, AIR looks at the specific cloud services used by specific companies. Because AIR has this type of detailed data for approximately 60,000 companies worldwide, it is able to perform detailed accumulation studies for all of them. In parallel, AIR is building a probabilistic model to arrive at distributions for annual frequencies of events, which industries are being targeted, the size and location of targeted companies, etc. Based on these distributions, AIR can create a stochastic catalog through which insurers could run their own portfolios to obtain information such as average annual loss and exceedance probability curves.

Christos Mitos and RMS apply a scenario-based modelling approach to affirmative exposures. In February of 2016, RMS released deterministic cyberattack scenarios that explicitly model five types of events: data exfiltration, mass DDoS attacks, cloud compromise, financial theft and cyber extortion. These plausible, yet extreme scenarios have been entered into the RMS cyber Accumulation Management System, which was developed in collaboration with eight partners, and with input from the Cambridge Centre for Risk Studies and Lloyd's, which has developed its own silent and



affirmative exposure scenarios. The RMS scenarios – which incorporate a series of three zero-day vulnerabilities that need to be exploited to trigger a large-scale incident – are not probabilistic in the same sense the term is understood in natural catastrophe (Nat Cat) or terrorism modelling.

Phil Holt states that, in recent years, Lloyd's has focused on working with the Lloyd's Market Association (LMA) to approach the problem of risk for every class of business. He breaks cyber loss potential into three broad categories. The first is data protection and data breach, for which the industry has a loss history that enables modelers to envision extreme scenarios. The second is cybercrime, which poses a somewhat greater challenge from an accumulation

point of view, since it is difficult to know how severe losses could be. The third, cyberterrorism, is probably the most difficult, and perhaps the most frightening, from a loss perspective: in the event of an attack on critical infrastructure, there is the potential for multiline aggregation and multiple involvements that are difficult to conceive of. In the context of attacking infrastructure, cyber could be considered a proximate cause of losses that the industry already knows how to quantify (the sinking of an oil tanker, for example). By compartmentalizing the problem into different components, we can better understand what we do and don't know, and where to apply our efforts to find a scenario that incorporates all of the potential lines of business and effects.

## CHALLENGES IN COLLECTING EXPOSURE DATA

Holt supports the view that the industry urgently needs to agree on a standardized way to structure and collect data. Further, any standards must be built on a framework that is flexible enough to accommodate changes resulting from unanticipated future realities.

“THE INDUSTRY URGENTLY NEEDS TO AGREE ON A STANDARDIZED WAY TO STRUCTURE AND COLLECT DATA. FURTHER, ANY STANDARDS MUST BE BUILT ON A FRAMEWORK THAT IS FLEXIBLE ENOUGH TO ACCOMMODATE CHANGES RESULTING FROM UNANTICIPATED FUTURE REALITIES.” *Phil Holt*

The AIR schema contains hundreds of data fields, although most are optional, and it may be decades before the preferred data is collected. According to Stransky, some of the key fields to capture are industry, revenue turnover and – in order to perform a detailed accumulation study – insured name. Without such data, an analysis is essentially market share based. Other preferred data include an insured's cloud vendor, payment process vendor, how many and what type of records a company has. In early 2016, AIR worked with RMS and Lloyd's to devise a common core data standard for cyber that lists approximately 20 recommended data fields that could realistically be collected.

Christos Mitas states that many RMS clients lack data beyond the sector and size of the insured. Whilst this is challenging, RMS have designed the model parameterizations focusing on these key variables. The RMS model collects jurisdiction data, which is important given the borderless nature of cyber, and necessary in order to perform accurate liability calculations for companies in different countries. He suggests that there needs to be a way to gauge the security of the network of every company that seeks to be insured. This would include data on the human-related vulnerabilities, perhaps even to the point of taking into account the psychology of social engineering. Ideally, insurers should have some concept of a company's network topology, as well as a valuation model for every intangible asset that constitutes the network. Credible third-party certifying organizations could collect such information, but modelers would also need to evaluate the methodologies and results of these providers. Holt adds that, from a claims perspective, third-party certification to help assess threat levels might be a viable alternative, given that insurers cannot measure such events independently due to the lack of disclosure legislation.


“IDEALLY, INSURERS SHOULD HAVE SOME CONCEPT OF A COMPANY'S NETWORK TOPOLOGY, AS WELL AS A VALUATION MODEL FOR EVERY INTANGIBLE ASSET THAT CONSTITUTES THE NETWORK.” *Christos Mitas*



Scott Stransky adds that the AIR database schema allows for the capture of NIST and ISO certification, as well as cyber Essentials (U.K.), but that this information is more qualitative, whereas quantitative data is more useful. AIR partnered with BitSight Technologies (U.S.) to assign a numerical value to its results to create a rating scale of 250-900, which was then correlated with breach probabilities. AIR found that companies with ratings under 500 are up to five times more likely to be breached than those with ratings over 700. This type of actionable information can be used in modelling.

All panelists agreed that the insurance industry would benefit from the existence of trusted, independent entities that would allow companies to anonymously report incidents and provide insurers the resulting anonymized

data to use for modelling. Stransky points out that NIST (National Institute of Standards and Technology) is planning to create a centralized repository of breach data in the U.S.



The insurance industry would benefit from the existence of trusted, independent entities that would allow companies to anonymously report incidents and provide insurers the resulting anonymized data to use for modelling.

---

## COVERAGE CHALLENGES AND SILENT EXPOSURE

Paul Nunn points out that, today, cyber insurance is bundled into existing products. He believes that in order for the risk to be better understood and quantified, specific cyber products are required in place of silent coverage within existing products.

Holt agrees that this is the greatest challenge. He states that Lloyd's Market offers affirmative cyber coverage that is well underwritten and based on a process of self-assessment and underwriter verification. This coverage is being accumulated in the way that would be expected from an account underwriting perspective, and it is backed by reinsurers who know the process. Silent coverage is a significant problem because the potential cost could be considerable unless a policy has sub limits and clear wording. Simply adding clear cyber exclusions to policies, which might be difficult in this market to do that anyway, is inadequate in itself, since our customers require coverage.

Christos Mitos states that RMS have been working with Cambridge on finalizing new scenarios based on the original affirmative scenarios created for its Cyber Accumulation Management System. RMS are also working with Cambridge on five loss processes quantifying cyber-physical attacks on silent exposures including commercial and residential property, marine, energy, industrial, facultative, specialty, casualty/liability, and others.

Scott Stransky finds silent cyber to one of the most frightening aspects of the cyber world today. He notes that insurers and reinsurers seem to be encountering a catch-22 situation with regard to modelling: if silent cyber is modelled then this could be interpreted as an acknowledgement that the policy might respond. The industry needs to work together to find a solution to this problem.

---

## VIABILITY OF PROBABILISTIC FRAMEWORKS FOR CYBER

Although probabilistic modelling is the standard for Nat Cat, Holt supports the view that it may be more appropriate to draw a parallel between cyber and terrorism models, given the fast rate at which cyber threats and risks are changing. He believes that probabilistic frameworks may never be stable enough to be practically useful in supporting the business decisions insurers need to make.

Stransky points out that there were similar concerns about hurricane modelling 20 or 30 years ago, emphasizing that, today, hurricane modelling is essential to insurance and reinsurance. He supports the view that the same will be true of cyber risk in a matter of years or decades. There are many techniques for adding new data to models and updating them in real time. For example, BitSight adjusts company ratings daily, information that can then be input into modelling.





This changes the risks in real time in a way that makes sense. While a cyber risk model would need to be updated more frequently than a traditional Nat Cat model, AIR does believe we will eventually get to a stable view of risk even for cyber.

Christos Mitas states that the way we understand the process of cyber risk modelling itself is more or less what is done with terrorism: we begin with a deterministic scenario, understand what the probable maximum loss should be, and add some variants. From there, we drill into the details of what produces the correlations between plausible, yet extreme scenarios and seek ways to incorporate probabilistic modelling. In the context of terrorism modelling, I have applied complexity theory, network theory, game theory and others to gain insight into some of the occurrence probabilities of major terrorism effects. There are currently studies being done using game theory to model terrorism risk in terms of a zero-sum stochastic game. The next steps for the industry are to pursue the silent exposure problem, and gain a more detailed understanding of the affirmative scenarios and the correlations produced by the different exposure elements we capture.

“THERE ARE CURRENTLY STUDIES BEING DONE USING GAME THEORY TO MODEL TERRORISM RISK IN TERMS OF A ZERO-SUM STOCHASTIC GAME”

*Christos Mitas*

Phil Holt proposes three different probabilistic distributions that the industry needs to be able to model for cyber: the probability of an attack (which could change daily depending on multiple factors), the probability of an organization's defenses preventing an attack, and how successful an attack is likely to be in terms of severity, or loss severity distribution. Although these categories clarify the problem, the solution remains elusive due to the rapidly changing cyber landscape. He suggests that, in the near future, probabilistic frameworks may support certain business decisions, and may help in differentiating between higher and lower risk. He doubts that probabilistic models for cyber will ever be stable enough to provide reasonable certainty, at least not used in isolation. However, he does believe we will have more useful models and tools in the near future.



# PROSPECTIVE ON DIGITAL INNOVATION

## Oussama Ammar, Founder, The Family



### OUSSAMA AMMAR

Founder  
The Family

**A traveller who feels at home anywhere he goes, from Paris to São Paulo to San Francisco, Oussama Ammar remembers each time he set out to make something new – all the way back to when he won his first computer at age 10 and started learning how to code.**

As a teenager, he was building online platforms for antique shops in his hometown; as a university student, he floated between law, philosophy, and the social sciences before deciding that school just wasn't for him. After a stint working in Hong Kong, he founded Hypios, a firm dedicated to solving complex R&D problems, but eventually the difficulties of building it into a viable business led him to settle in Silicon Valley and start putting together investment deals for other entrepreneurs. Now, his goal at TheFamily is to find those founders who are able to put their results above their intelligence, those who seek big markets with big problems, and those who are capable of building empires, and he knows that any single idea is just an infinitesimal part of doing that.

The Family is an investment firm operating in Paris, London and Berlin. We invest as early as possible in startups and try to reinvest in every round of those that are successful. Our aim is to grow big companies; the kinds of companies that could kill traditional companies like (re)insurance companies.

These days, it is impossible to accurately judge a startup idea because most of them seem weak in the beginning. However, if you evaluate startups from an idea perspective, you are missing what makes them important: the execution capability of the founders. Good founders make all the difference because they can implement their ideas better than their competition can.

“EXECUTION IS UNPREDICTABLE,  
AND MOST TRADITIONAL MARKET  
EVALUATION TOOLS, LIKE  
BUSINESS PLANS, DO NOT WORK  
TODAY.”

We have gone from a linear world, where predictability can be modelled, to an exponential world, where we humans struggle to grasp outcomes. And we always tend to follow the same pattern in this context: at the beginning we overestimate potential, while later we underestimate it.

There is much talk today about “digital transition,” and we are no longer talking about processes that occur over time. Today we are seeing “quantum” changes: some time, somewhere, in some industry, it is entirely possible that total transformation occurs. We are living through a paradigm shift.

How do humans react to changing paradigms? The first person who suggested to doctors that they wash their hands was a Frenchman. But that visionary doctor was sent to jail. When he still wouldn't relent, he was sent to a psychiatric hospital and then he was lobotomized. This is how people can react to changing paradigms. By telling doctors people will die if they don't wash their hands, the implication is that they have been killing people for decades. Our minds resist confronting realities like this.



## CASE STUDY: UBER

It is hard to predict whether a startup will succeed. Even the most successful of them rarely look impressive in the first year or two.

When Uber sought its first funding round, it was offering 5% of the company for USD 50,000. But when leaving for a long time in France, which has a particularly strong taxi culture, the taxi industry seemed really unassailable. At today's valuation, that translates to a loss of USD 700 million.

Many people think that Uber's USD 60 billion valuation is excessive. Yet the following numbers speak volumes:

1. In 2008, when Uber was launched, the size of the taxi industry in San Francisco was USD 508 million. By December of 2015, it was USD 67 million. In seven years, the industry lost 90% of its value. Yellow Cab, the oldest California taxi company, which had been owned by the same family for five generations since the 19th century, filed Chapter 11 bankruptcy! In its first year in San Francisco, Uber made USD 1 million. Last year, it made USD 1 billion in San Francisco alone. Uber destroyed the biggest incumbent and doubled the size of the market.
2. Uber achieved this with a total investment (operations plus overhead divided by every city in the world where they operate) in San Francisco of about USD 60 million. This investment produced a USD 1 billion company that generated roughly USD 400 million in profit for Uber in San Francisco alone.
3. In the last six months, Uber has hired an unprecedented 1 million drivers worldwide.

Five years ago, we could not have imagined growth at such a scale. And yet, this is no guarantee that Uber is a

successful company, or that it will survive. In today's world, the age-old belief that "the earlier the investment, the greater the risk, but also the greater the reward" is no longer true. In my opinion, investing in Uber now, with its USD 60 billion valuation, would be a bargain. It would also be a very high-risk, early-stage investment. However, we are not trained to understand that as a financial model. We are trained that if a company is eight years old and has raised USD 90 million, the risk should be lower. But there are three main reasons why, even today, Uber is still a risk:

1. Uber set out to create a monopoly rather than simply to be the market leader. This is the biggest difference between historical companies and companies of the startup era. Startups today try to build monopolies with a degree of hubris that is quite new in the history of business.
2. Uber is not competing against the taxi industry. It is competing against cities, governments and car manufacturers.
3. Uber is also competing against technological shift. The same thing Uber is doing in terms of disruption, and that at a very fast pace, can happen to them. If Google or General Motors were to launch self-driving cars, they would be a major threat to Uber.

"TODAY, COMPETITION IS NOT STABILIZING AT SCALE, IT IS INCREASING AT SCALE."

## CASE STUDY: GOOGLE

It is unlikely that people think Google could be bankrupt in five years. When analyzing numbers on a "temporis" basis, which means not looking at user groups as a whole, but at users who behave in certain ways at the same time, you realize that most early adopters of Google do not use it anymore. Most users who once searched for products on Google now use the Amazon app for example. Those who once purchased train and plane tickets through Google may now use many other app.

Google remains in a strategic position due to revenues that are increasing quarterly, thanks to the advertising industry.

Because the ad industry was slow to transition from traditional to digital advertising, Google faces tremendous growth, even though its core function – search – is declining. This case reveals the gap between the traditional and the new economy.

Google understands this better than anyone, which is why the company built Alphabet. It was not for financial discipline, but to make sure that everyone at Google internalizes the fact that the future of Google is not google.com.



## CASE STUDY: THE MUSIC INDUSTRY

The year 2008 was the highest-earning year in the history of the music industry, with USD 55 billion in revenues worldwide. Last year, the total revenues were USD 7 billion. In 2008, Spotify did not exist, and last year it made USD 1 billion – almost 20% of the entire industry’s revenues today. This is a very interesting case to look at.

The changes are symptomatic of a hacker-driven industry: not in terms of information security but, rather, of mindset. The top startups that killed the music industry – Napster, Spotify, Deezer, etc. – were built by teenagers. “Pirates” who want to be able to express their freedom over rights, content and publicity.

Professional music artists today bemoan the passing of an idyllic world of magical, beautiful creation, and complain that they can no longer create (which really means they

can no longer make billions from the past, for example, Michael Jackson released his hit “Billie Jean,” which sold him 80 million albums – a world record – and made him USD 1.2 billion. In contrast, four years ago, the “Gangnam Style” video uploaded to YouTube by an unknown Korean man got 4 billion views and earned the artist USD 12 million. The entire world was singing in Korean.

There is one figure that suggest we are on the right side of this phenomenon: last year, 165 thousand people in the world made more than USD 40,000 from publishing their music online. Music was once an elite thing: Michael Jackson had the right producers, distributors, marketing, and so on. Today it is an industry that is no longer blockbuster driven, and has become so “long tail” that anyone has the chance to make a living from their passion.

## DISRUPTION IS INEVITABLE

What happened to music will happen to every industry. It is the natural movement of the economy, and the Internet makes it possible. This is what big companies are struggling to understand. The next big companies will not build products but, rather, they will build infrastructures and platforms that make it possible to produce products on a long-tail basis.

But what people don’t understand about the entrepreneurial shift is that we are all eager for this transformation,

despite the conflict that comes with it. Inside each of us there is a consumer side and an employee/owner side. The consumer wants everything cheaper, better, faster. We do not care about the human cost – that some humans may be hurt by the transformation. Take, for example, the robot in Japan that produces a better cancer diagnosis than any doctor in the world. If you had cancer, would you be more concerned about your doctor being unemployed, or your survival thanks to software?





---

## IN CONCLUSION

People tend to see the shift we are experiencing as a technological movement, but it is not. Big company usually do the same mistake and they hand the digital transformation off to their IT department. But computers are only tools.

---

**“THE TRANSFORMATION STARTS  
WITH THE CONSUMERS”**

---

There are two ways to look at this new phenomenon:

- ♦ The conservative view is that technology is to blame for people’s “crazy” behavior.

Or

- ♦ in my view, today people are empowered to a degree they have always dreamed of being, and now they can express it on powerful social medias. This sense of empowerment is a universal desire. And because it is universal, technology is turning people into a commodity. **We are entering a niche commoditization business era.** It is foolish to continue to think that centralization and outside commodity strategies work. The (re)insurance industry should be ready for a huge transformation that is definitely coming.



To request an electronic copy, please email : [scorglobalpc@scor.com](mailto:scorglobalpc@scor.com)

All rights reserved. No part of this publication may be reproduced in any form without prior permission of the publisher. SCOR has made all reasonable efforts to ensure that information provided through its publications is accurate at the time of inclusion and accepts no liability for inaccuracies or omissions.



Editor: SCOR Global P&C  
Strategy & Development  
[scorglobalpc@scor.com](mailto:scorglobalpc@scor.com)

**No. ISSN 1638-3133**  
**Focus #22 - APRIL 2017**

SCOR, 5 avenue Kléber  
75795 Paris Cedex 16 - France  
[www.scor.com](http://www.scor.com)

**SCOR** | P&C  
The Art & Science of Risk

