L'Attuario nella gestione dei rischi per le imprese e per la collettività

Cyber Risk management: identificare e gestire le nuove forme di rischi operativi

I modelli di analisi nella gestione dei rischi:

lo stato dell'arte della ricerca a supporto alla professione

16 giugno 2016

Cyber Risk management: le nuove forme di rischi operativi

Oggi giorno i **rischi informatici** rappresentano una delle minacce più difficili da affrontare e in grado di generare ricadute economiche e di immagine estremamente negative per le imprese. Cosa sono e come è possibile affrontarli?

La globalizzazione, caratterizzata dall'apertura dei mercati e dal venire meno dei confini spazio-temporali, ha incentivato l'utilizzo delle tecnologie informatiche da parte delle imprese, sempre più alla ricerca di strumenti in grado di assicurare una **comunicazione** e un **trasferimento dati** in **tempo reale** con soggetti localizzati in ogni parte del mondo.

Cyber Risk management: le nuove forme di rischi operativi

La rapida e costante evoluzione delle tecnologie dell'informazione e della comunicazione (ICT) ha, inoltre, reso la capacità di saper raccogliere, interpretare, trattare, **conservare** e **proteggere** i dati di fondamentale importanza per le imprese.

In questo contesto, l'adozione di efficienti ed efficaci strumenti di gestione del rischio informatico – **cyber risk management** – assume rilevanza cruciale, in quanto da essa possono dipendere le sorti stesse dell'impresa.

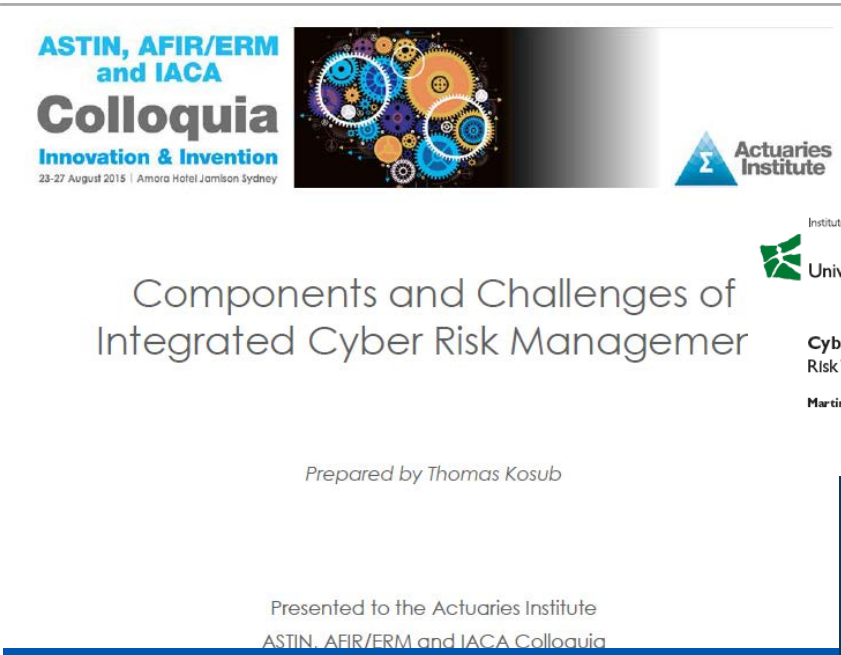
Cyber Risk management: le nuove forme di rischi operativi

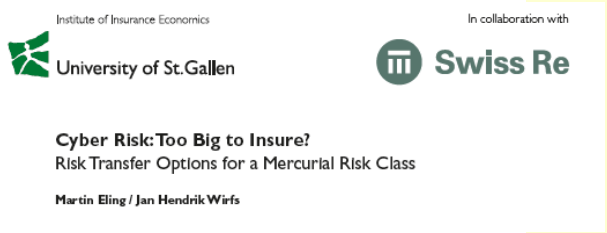
Trasferire il rischio: questa, tra le diverse possibili azioni previste nella gestione di un rischio, è quella che tradizionalmente crea maggiori incertezze quando si parla di sicurezza delle informazioni.

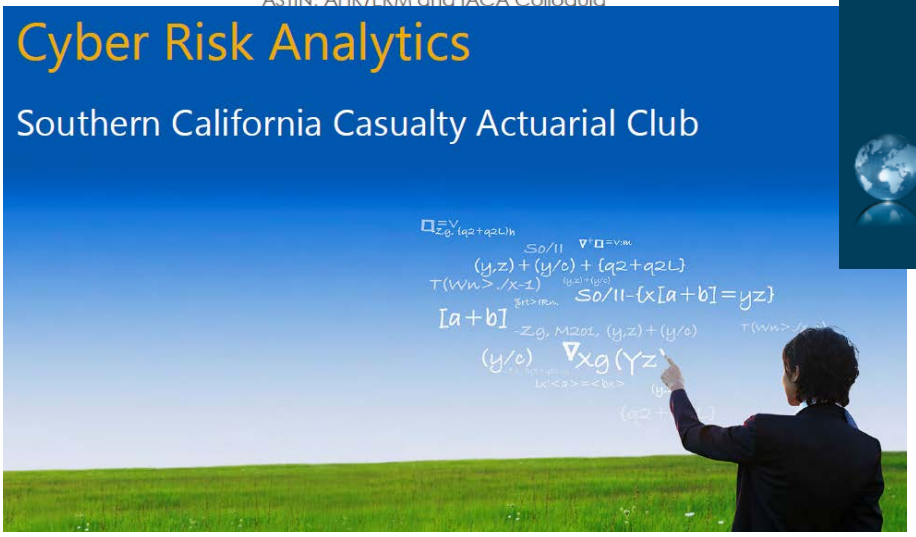
Assicurare i beni del magazzino o l'edificio da rischi quali furto o incendio è una delle azioni che le aziende compiono da ben prima dell'apparizione degli strumenti informatici. **Stimare l'impatto che questi avvenimenti possono comportare per la gestione delle informazioni è molto diverso**.

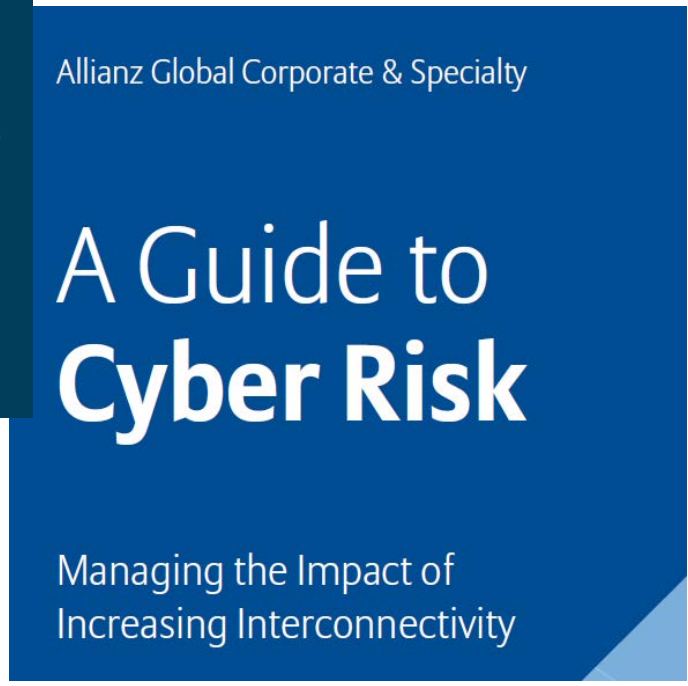
Quasi tutte le aziende posseggono una polizza incendio. Se a bruciare però è la sala server, vedersi rifondere il mero valore dell'hardware…
E come assicurare un furto di dati?

Cyber Risk management: le nuove forme di rischi operativi









IAIS - International Association of Insurance Supervisors

ISSUES PAPER ON CYBER RISK
TO THE INSURANCE SECTOR
DRAFT 14 APRIL 2016

IAIS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

Concern over **cybersecurity is growing across all sectors of the global economy**, as cyber risks have grown and cyber criminals have become increasingly sophisticated. For **insurers, cybersecurity incidents can harm the ability to conduct business, compromise the protection of commercial and personal data, and undermine confidence in the sector**. The IAIS has noted that the level of awareness of cyber threats and cybersecurity within the insurance sector, as well as supervisory approaches to combat the risks, appear to vary across jurisdictions.

These factors prompted the IAIS to consider the area of cybersecurity in the insurance sector, **including the involvement of insurance supervisors in assessing and promoting the mitigation of cyber risk**. While many of the most widely publicised cybersecurity incidents involving consumer data have affected retailers, companies in the financial services sector, including insurers, have been victimised as well.

IAIS - International Association of Insurance Supervisors

All insurers, regardless of size, complexity, or lines of business, **collect, store, and share with various third-parties** (e.g., service providers, reinsurers) **substantial amounts of private and confidential policyholder information**, including in some instances sensitive health-related information.

Information obtained from insurers through cyber crime may be used for financial gain through extortion, identity theft, misappropriation of intellectual property, or other criminal activities. Exposure of private data can potentially result in severe and lingering harm for the affected policyholders, as well as reputational damage to insurer sector participants.

IAIS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

IAIS - International Association of Insurance Supervisors

The objectives of the Issues Paper are to **raise awareness** for **insurers and supervisors of the challenges presented by cyber risk**, including current and contemplated supervisory approaches for addressing these risks. As an Issues Paper, it provides background, describes current practices, identifies examples, and explores related regulatory and supervisory issues and challenges.

The paper focuses on **cyber risk to the insurance sector and the mitigation of such risks**, but does not cover IT security risks more broadly. It also does not specifically address insurers' underwriting of cyber risk (i.e., cyber insurance) or risks arising from cybersecurity incidents involving supervisors.

IAIS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

IAIS - International Association of Insurance Supervisors

There is **no standardised definition** of the term "cyber risk."

The CRO Forum has broadly described "cyber risk" to mean: "*Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks*. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or governments."

IAIS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

IAIS - International Association of Insurance Supervisors

Cyber risk presents a growing challenge for the insurance sector, and one which, under the Insurance Core Principles, **supervisors are obliged to address**. Insurers collect, store, and manage substantial volumes of confidential personal and commercial information. Because of these reservoirs of data, insurers are prime targets for cyber criminals who seek information that later can be used for financial gain through extortion, identity theft, or other criminal activities. In addition, **because insurers are significant contributors to the global financial sector, interruptions of insurers' systems due to cybersecurity incidents may have far-reaching implications**.

IAIS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

IAIS - International Association of Insurance Supervisors

Given past experience and forecasted trends, **cyber risks and the impact of cyber incidents will continue to grow**. Supervisors should seek to increase their understanding of cyber risk and their supervisory capabilities concerning the insurance sector's cyber resilience. Such supervisory focus might appropriately include, but should not be limited to, **insurers' awareness of cyber risk** and cyber resilience, and insurers' development and implementation of policies, procedures, and technology to **increase cyber resilience**, including the implications of outsourcing and other third-party connections on cyber resilience.

IAIS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

EU General Data Protection Regulation 2016

Il 4 Maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il "Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo **alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

Il Regolamento entrerà in vigore il 25 Maggio 2016 e sarà concretamente operativo nei Paesi UE a decorrere dal 25 maggio 2018, lasciando a tutti i soggetti interessati un biennio di tempo per gli adeguamenti necessari alle proprie politiche del trattamento dei dati.

EU General Data Protection Regulation 2016

Le aziende devono prestare particolare attenzione all'analisi dei trattamenti, identificazione dei rischi e contromisure per mitigarli al fine di 'disegnare' processi privacy aziendali corretti ed efficaci.

Introduce un **meccanismo sanzionatorio senza precedenti**, con sanzioni fino a 20 milioni di euro o fino al 4% del fatturato annuale globale di gruppo per le multinazionali.

La materia della **protezione dei dati** diventa a questo **punto centrale** in tutte le politiche di compliance aziendale, ma anche elemento cruciale delle politiche produttive e di business.

Allianz Risk Barometer 2016

Cyber risk appears in many forms, all of which can represent major threats to business. Companies increasingly face new exposures, including first-and third-party damage, business interruption and regulatory consequences.

It is estimated that cyber-crime alone **costs the global economy approximately $445bn** a year with the world's largest economies accounting for around half of this. The threat posed by such incidents is expected to increase further during 2016.

This increasing risk is reflected in the Risk Barometer with cyber incidents (cyber-crime, data breaches, IT failures) gaining 11 percentage points year-on-year to move into the top three risks for the first time (28%). Three years ago this peril ranked just 15th (6%).

Allianz Risk Barometer 2016

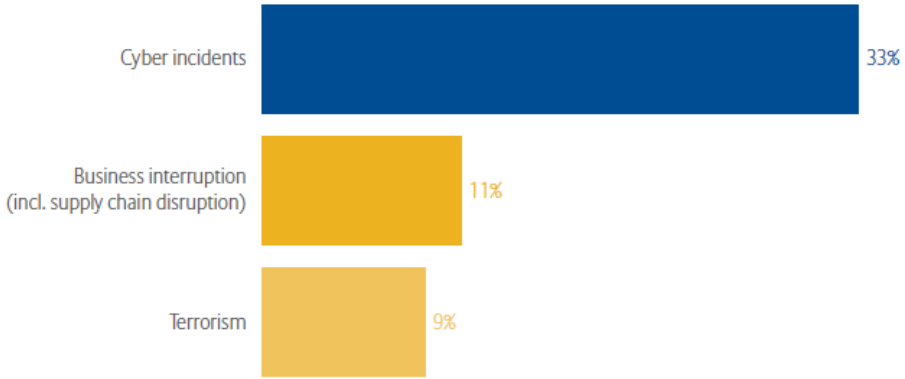
What are the main causes of economic loss after a cyber incident?

Source: Allianz Global Corporate & Specialty. Figures represent the percentage of participants who responded (281). Up to three answers possible.

What is preventing companies from being better prepared against cyber risks?

Source: Allianz Global Corporate & Specialty. Figures represent the percentage of participants who responded (281). Up to three answers possible.

What are the top emerging risks for the long-term future (10yrs+)



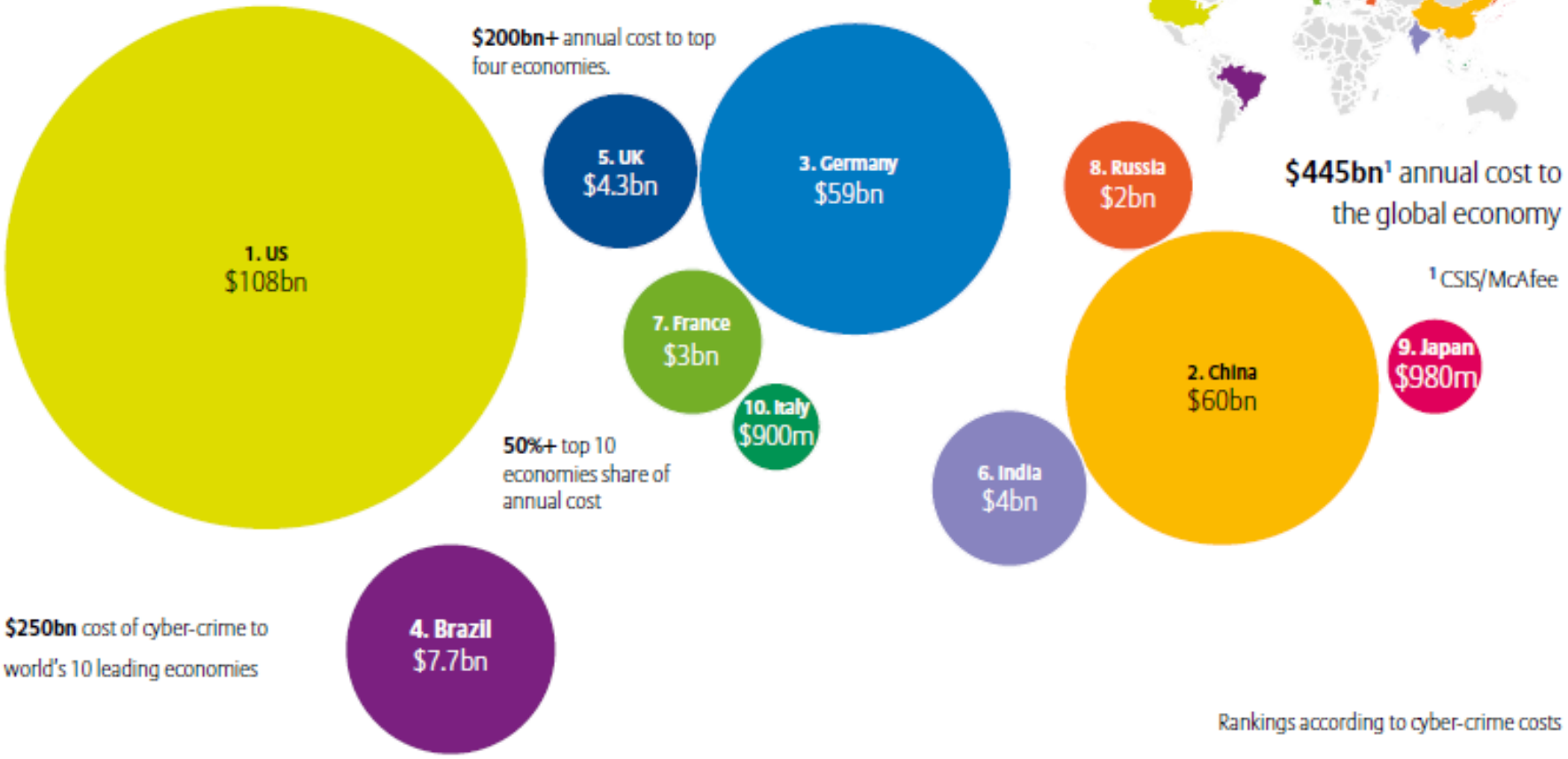
Cyber incidents is the top long-term risk for businesses. Impact of digitalization and new technology also feature in the top 10 risks identified.

Source: Allianz Global Corporate & Specialty. Figures represent the percentage of participants (824) who selected that specific risk. Up to three answers possible.

The Cyber Risk Landscape today

How much does **cyber-crime** cost the world's leading 10 economies?

This **AGCS** atlas examines the estimated total cost to the global economy from cyber-crime per year, with a particular focus on the impact on the world's top 10 economies, according to GDP.



The Cyber Risk Landscape today

Country Ranking by GDP[1]		Cyber-crime as a % of GDP[2]	Estimated cost[3]
1 US	$16.8trn	.64%	$108bn
2 China	$9.5trn	.63%	$60bn
3 Japan	$4.9trn	.02%	$980m
4 Germany	$3.7trn	1.60%	$59bn
5 France	$2.8trn	.11%	$3bn
6 UK	$2.7trn	.16%	$4.3bn
7 Brazil	$2.4trn	.32%	$7.7bn
8 Russia	$2.1trn	.10%	$2bn
9 Italy	$2.1trn	.04%	$900m
10 India	$1.9trn	.21%	$4bn

Sources: [1]World Bank (2013) [2]Net Losses: Estimating the Global Cost of Cyber-Crime, CSIS/McAfee [3]Allianz Global Corporate & Specialty

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

Growth in the US is already underway, driven by data protection regulation. Legislative developments and increasing levels of liability will help growth accelerate elsewhere, as will a growing number of small- to medium-sized enterprises (SMEs) seeking cover.

Dalla polizza tradizionale alla polizza cyber

Le polizze cyber presenti oggi sul **mercato italiano** sono **poche** e sono piuttosto diverse tra di loro.

Tipicamente ci troviamo davanti ad una serie di sezioni, attivabili o meno, che prendono in considerazione:

- *Danni occorsi ai beni ICT (macchine) ed ai dati propri o di Terzi*
- *Danni legati alla violazione della Privacy (dati personali e/o commerciali) propria o di Terzi*
- *Danni causati dal crimine informatico e quelli da guasto ed errore umano (di dipendente o terzi)*
- *Danni che impattano sull'attività aziendale (interruzione di esercizio, richieste di risarcimento da parte di terzi.*

Risarcire una serie di costi connessi a questi danni non è sempre previsto dalle polizze tradizionali.

Cyber danni

Danni materiali diretti: riguardano i danni (distruzione parziale o totale, furto) subiti da beni materiali (un server, la fibra ottica, i PC..) e direttamente causati dall'evento che sarà normalmente di natura tradizionale (rientrano già nella polizza incendio, nella polizza trasporti, nella polizza «all risks») e nella polizza «elettronica»

Danni materiali indiretti (o consequenziali) : si tratta ugualmente di danni a beni materiali, ma conseguenza di danni diretti (esempio un fenomeno elettrico che abbia danneggiato una scheda, il cui malfunzionamento danneggi a sua volta la macchina di produzione da essa controllata

Danni immateriali diretti ed indiretti: sono tutti quelli che non riguardano la materialità delle cose assicurate e che sono conseguenza di un evento garantito in polizza (l'evento dannoso distrugge o compromette l'integrità di un software ovvero rende indisponibili i dati aziendali)

Cyber danni

Le polizze cyber risarciscono certamente i costi sostenuti per la sostituzione del software e le operazioni di ripristino e di ricostruzione dei dati. Ma se questo non fosse possibile?

Quantificare il valore di un database è un'operazione di una certa complessità (in questo senso una preventiva analisi degli asset immateriali, l'adozione documentata di tecnologie/procedure per circoscrivere, valorizzare, proteggere…)

Alle classi di danni sono connessi **costi e spese di vario genere** volte ad indagare le cause, le eventuali responsabilità ed a ripristinare lo stato dell'arte (causa, tempo di ripristino, costi di ripristino, perdite di profitto, stima perdita di quote di mercato)

SAS OpRisk Global Data

The database consists of 26,541 incidents of operational loss that were reported between January 1995 and March 2014. The incidents occurred all over the world and each loss is categorized in accordance with the Basel II event and effect classification standard (BIS, 2006).

Table 4 Losses per Risk Type (in million US$)

Category	N	Mean	Std. dev.	Min.	Quantiles			VaR	TVaR	Max.
					25%	50%	75%	(95%)	(95%)	
Panel A: Cyber versus non-cyber risk										
Cyber risk	1,579	43.49	426.36	0.10	0.43	1.53	7.43	100.55	730.52	14,589
Non-cyber risk	24,962	98.52	1,154.39	0.10	1.39	5.09	24.45	271.60	1,565.81	97,687
Panel B: Cyber risk subcategories										
Actions of people	1,203	42.66	475.53	0.10	0.42	1.35	5.39	77.75	743.20	14,589
Systems and technical failure	212	45.32	141.23	0.10	0.57	4.78	26.98	232.56	485.10	1,668
Failed internal processes	108	15.12	48.96	0.10	0.36	1.32	7.45	65.62	179.91	372
External events	56	109.12	431.92	0.10	1.04	4.25	19.53	331.06	1,585.58	2,949

SAS OpRisk Global Data

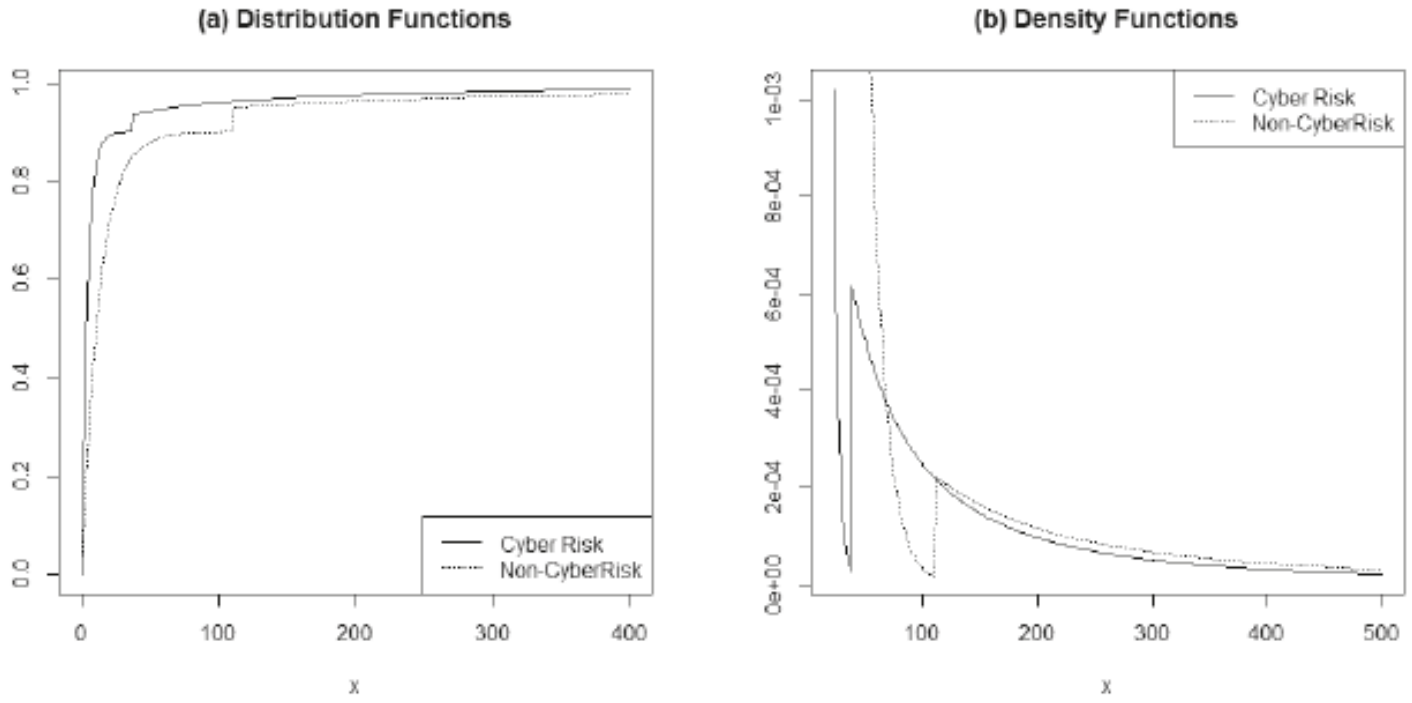
Table D1 Risk Measurement

Model	Cyber Risk (N = 1,579)		Non-Cyber Risk (N = 24,962)	
	VaR	TVaR	VaR	TVaR
POT (threshold of 90%)	**104.63**	1,720.03	226.78	4,565.33
Exponential	130.20	173.72	295.51	393.73
Gamma	213.03	352.20	474.48	772.17
GPD	**94.35**	222,554.60	**237.39**	24,730.33
Log-normal	63.15	238.18	206.62	851.67
Weibull	88.61	196.32	232.64	496.80
Empirical	100.55	730.52	271.60	1,565.81

Note: Value at risk (VaR) and tail value at risk (TVaR) at 95% confidence level.

SAS OpRisk Global Data

Figure D1 Estimated Distribution and Density Function



Conclusioni

Il tema è di grande attualità e la gestione di molti aspetti è oggetto di discussioni strategiche sia nel mondo assicurativo che nel mondo delle aziende.

Un certo livello di rischio andrà accettato, o perché davvero accettabile o perché non si può fare diversamente ma **fondamentale** è la **conoscenza del problema** per non farsi sorprendere dall'emergenza.

Grazie per l'attenzione

Cyber Risk management: le nuove forme di rischi operativi

Marco Pirra

marco.pirra@italian-actuaries.org

marco.pirra@unical.it