
Estratto

Estratto da un prodotto
in vendita su **ShopWKI**,
il negozio online di
Wolters Kluwer Italia

Vai alla scheda →

Wolters Kluwer opera nel mercato dell'editoria
professionale, del software, della formazione
e dei servizi con i marchi: IPSOA, CEDAM,
Altalex, UTET Giuridica, il fisco.



1. REVIEW DELLA LETTERATURA SU CYBER INSURANCE: CONCETTI CHIAVE E PROSPETTIVE FUTURE

di Patrizia Tettamanzi e Michael Murgolo

1.1.	Introduzione	3
1.2.	<i>Background</i> sul tema e studi correnti	4
1.3.	Metodologia di ricerca	9
1.4.	Fase 1 di 3: <i>Review</i> sistematica della letteratura (SLR)	9
1.5.	Fase 2 di 3: Analisi bibliografica di <i>network</i> (BNA)	10
1.6.	Fase 3 di 3: Tecniche addizionali di analisi (AAT)	13
1.6.1.	Analisi dello <i>score</i> citazionale (CSA)	13
1.6.2.	<i>Keyword Network Analysis</i> (KNA)	16
	1.6.2.1. <i>Co-occurrence analysis</i> sulle <i>keywords</i> degli autori	16
	1.6.2.2. Algoritmo della <i>burst detection</i> di <i>kleinberg</i>	17
1.7.	Identificazione di nuove direzioni di ricerca	19
1.8.	Discussione finale e conclusioni	20

2. LA STORIA E L'EVOLUZIONE DELL' ASSICURAZIONE CYBER

di Rossella Bollini

2.1.	Genesi del mercato assicurativo <i>cyber</i> : l'insorgere della domanda e contesto di riferimento	29
2.2.	Le prime polizze <i>cyber</i> : caratteristiche e <i>gaps</i>	33
2.3.	<i>Milestones</i> e sviluppi successivi	36
2.4.	Sinistri e reazione di mercato	44
2.5.	Avvento di nuove tecnologie e conseguente impatto	46
2.6.	Prospettive future	53

3. LA TECNOLOGIA E IL CYBER RISK: PRINCIPALI THREATS E RISCHI INFORMATICI

di Paolo Colombo e Rebecca Platini

3.1.	Il <i>cyber risk</i> in un panorama delle minacce in continua evoluzione	59
3.2.	Attori malevoli e i loro obiettivi	62
3.2.1.	Il <i>ransomware</i> come modello di <i>business cyber-criminale</i>	62
	3.2.1.1. LockBit 3.0: l' <i>industry-leader</i> del <i>Ransomware-as-a-Service</i> (RaaS)	66
	3.2.1.2. Scattered Spider e ALPHV: una nuova collaborazione tra avversari finanziariamente motivati	68

3.2.2.	Gruppi <i>state-sponsored</i> e il <i>cyber-spionaggio</i>	69
3.2.2.1.	<i>Sandworm</i> e gli attacchi alle infrastrutture critiche ucraine	71
3.2.2.2.	Le operazioni di influenza sulle elezioni politiche del 2024	72
3.2.3.	<i>Hacktivismo</i> : nuove frontiere dei conflitti nel cyberspazio	75
3.2.3.1.	Nuovi sviluppi dell' <i>hacktivismo</i> nel conflitto Russo-Ucraino: un precedente per il futuro	76
3.3.	Principali tecniche di attacco e vulnerabilità	78
3.3.1.	<i>Malware</i>	78
3.3.2.	Ingegneria sociale (<i>Social engineering</i>)	80
3.3.3.	Attacchi alla <i>Supply chain</i>	82
3.3.4.	Vulnerabilità di sicurezza	83
3.3.5.	Il potenziale dell'Intelligenza Artificiale: minaccia o soluzione?	84
3.4.	Nuove frontiere e sfide emergenti: ulteriori sviluppi tecnologici e possibili nuove minacce	88

4. IL CONTRATTO DI ASSICURAZIONE CYBER: PECULIARITÀ E FUNZIONE

di Nicolò d'Elia e Marianna Scardia

4.1.	Verso la <i>cyber</i> resilienza: un sistema complesso di fonti	93
4.1.1.	Le fonti europee	93
4.1.1.1.	GDPR	93
4.1.1.2.	NIS e NIS2	94
4.1.1.3.	<i>Cyber Resilience Act</i>	96
4.1.1.4.	DORA	96
4.1.2.	Le fonti nazionali	96
4.2.	Il contratto di assicurazione cyber: la sua funzione di gestione del rischio e le incompatibilità con i modelli assicurativi tradizionali	97
4.2.1.	L'oggetto e la classificazione dell'assicurazione <i>cyber</i>	97
4.2.2.	La funzione del contratto assicurativo <i>cyber</i>	98
4.2.3.	Dichiarazioni inesatte e reticenze dell'assicurato (artt. 1892 e 1893 c.c.): insufficienza del questionario contenuto nel modulo di proposta	99
4.2.4.	I limiti alla copertura assicurativa	101
4.2.5.	Gli obblighi di avviso e di salvataggio	102
4.3.	Il ruolo del contratto di assicurazione <i>cyber</i> nel contesto di un <i>data breach</i>	103
4.3.1.	Il <i>data breach</i>	103

4.3.2.	Gli obblighi di notifica al Garante <i>Privacy</i>	103
4.3.3.	Le potenziali conseguenze dannose di un <i>data breach</i> sui diritti degli interessati.....	106
4.3.4.	Il contratto di assicurazione <i>cyber</i> nella mitigazione dei danni conseguenti ad una violazione di dati personali	109
5.	IL MERCATO DELLA CYBER INSURANCE: OFFERTA, DOMANDA E DINAMICHE	
	<i>di Chiara Gatti</i>	
5.1.	L'immanente necessità di stabilità	113
5.2.	Il ruolo delle Compagnie di assicurazioni attive nel mercato della <i>Cyber Insurance</i>	113
5.3.	Lo Stato di diffusione dell'assicurazione <i>cyber</i> . <i>Protection Gap</i> e Domanda.....	114
5.4.	La peculiarità del <i>Cyber risk</i> per il mercato assicurativo.....	119
5.4.1.	Il rischio contagio come variabile nei modelli di <i>pricing</i>	121
5.4.2.	Il Rischio Catastrofale	122
	5.4.2.1. Incidente da <i>IT service provider</i>	123
	5.4.2.2. Interruzioni delle infrastrutture critiche..	124
	5.4.2.3. Attacchi su larga scala nell'ambito di una guerra informatica.....	125
	5.4.2.4. Violazione di dati personali	127
5.5.	L'offerta di polizze <i>Cyber</i>	129
5.5.1.	Servizi di <i>Risk Mitigation</i> nel mercato della <i>cyber insurance</i>	131
5.5.2.	Scenari e Perdite	132
5.5.3.	I <i>threat actors</i>	136
5.5.4.	I limiti delle coperture assicurative	136
5.6.	Tendenze emergenti	138
5.7.	La sottoscrizione di rischi <i>cyber</i>	139
5.7.1.	L' <i>impact underwriting</i> dei controlli	141
5.7.2.	I controlli dei Sistemi <i>end of life</i>	142
5.7.3.	<i>Digital supply chain cyber risk management</i>	142
5.7.4.	Le asimmetrie informative nel processo di <i>cyber underwriting</i>	143
5.8.	Il rischio di sottoscrizione <i>cyber</i>	145
5.9.	Metodi alternativi di trasferimento del rischio informatico: Parametriche, Mutue, <i>Cat-bond</i>	146
5.10.	Un approccio a un approccio a scala per i rischi informatici sistematici.....	149
5.11.	Il contributo della <i>Cyber Insurance</i> alla <i>Cyber Resilienza</i>	150

6. TECNOLOGIE EMERGENTI E L'IMPATTO SULL'ASSICURAZIONE CYBER*di Emanuele Gagliano*

6.1.	Introduzione	155
6.2.	Valutazione iniziale del rischio con tecnologie emergenti	156
6.2.1.	Scansione informatica esterna e rilevazione di vulnerabilità	156
6.2.2.	Ricerca di credenziali compromesse e analisi del <i>dark web</i>	156
6.2.3.	Identificazione di siti internet “copia” e rischi di <i>phishing</i>	157
6.2.4.	Ruolo dell'intelligenza artificiale generativa nella semplificazione dei rischi tecnici	157
6.3.	Gestione continuativa del rischio durante la vita della polizza ..	158
6.3.1.	Monitoraggio e <i>Vulnerability Management</i> continuo ..	158
6.3.2.	L'uso di soluzioni di <i>Extended Detection and Response</i> (XDR)	159
6.3.3.	Strategie di <i>backup</i> e resilienza ai <i>ransomware</i>	159
6.3.4.	Il ruolo dell'intelligenza artificiale nella gestione dinamica del rischio	160
6.4.	Paralleli con l'assicurazione automobilistica	160
6.4.1.	Tecnologie di monitoraggio e personalizzazione delle polizze	160
6.4.2.	Applicazione nel contesto <i>cyber</i>	161
6.4.3.	Raccolta dati e prevenzione	161
6.4.4.	Impatto sui rinnovi delle polizze	161
6.5.	Servizi di <i>Incident Response</i> e il loro ruolo	162
6.5.1.	Definizione e importanza dei servizi di <i>Incident Response</i>	162
6.5.2.	Ruolo nella gestione degli incidenti	162
6.5.3.	Prevenzione e preparazione	163
6.5.4.	Impatto sui rinnovi delle polizze e sulla gestione del rischio	163
6.5.5.	Collaborazione tra assicuratori e servizi di IR	164
6.6.	Conclusioni	165
6.6.1.	Un approccio olistico alla <i>cybersecurity</i>	165
6.6.2.	L'Importanza della valutazione continua del rischio ..	165
6.6.3.	Analisi delle terze parti	166
6.6.4.	Servizi di <i>Incident Response</i> : un elemento chiave	166
6.6.5.	L'uso dell'AI e <i>Machine learning</i> per la valutazione del rischio	167
6.6.6.	Normative e certificazioni di sicurezza	167

6.6.7.	Nuove frontiere: <i>blockchain, quantum computing e 5G</i>	167
6.6.8.	Un nuovo paradigma per un futuro sicuro	168
6.6.9.	Prospettive future ed evoluzione del settore	169
7. LA VALUTAZIONE PRATICA DEL RISCHIO PER LA CYBER INSURANCE		
<i>di Emanuele Capra</i>		
7.1.	Il punto di partenza: la mia esperienza	173
7.2.	Il <i>cyber risk management</i>	173
7.2.1.	Le fasi del processo	173
7.2.2.	La fase della valutazione del rischio: il passaggio più importante	174
7.2.3.	Metodologie e modelli per la valutazione del rischio <i>cyber</i>	174
7.2.4.	Valutazione del rischio <i>cyber</i> : alcuni modelli interessanti	175
7.2.5.	La gestione dei rischi HSE: un approccio da seguire anche per la <i>cybersecurity</i>	182
7.2.6.	Il processo assuntivo delle polizze <i>cyber</i>	183
7.3.	Le difficoltà nella valutazione del rischio <i>cyber</i>	185
7.3.1.	Le difficoltà della percezione del rischio reale da parte della Domanda	185
7.3.2.	La scarsa consapevolezza del rischio <i>cyber</i> da parte della Domanda	187
7.3.3.	Le compagnie assicurative: evoluzione in corso	188
7.3.4.	Il differenziale informativo ostacola la valutazione dei rischi	189
7.4.	Il miglioramento della valutazione dei rischi <i>cyber</i> per avviare il processo di <i>cyber risk management</i>	190
7.4.1.	Prima tappa: aumentare la consapevolezza partendo dai danni potenziali	190
7.4.2.	Seconda tappa: migliorare ulteriormente alcuni processi assicurativi	192
7.4.3.	Terza tappa: integrare il questionario assicurativo con un checkup preliminare finalizzato a dare consapevolezza al cliente	194
7.4.4.	La quarta tappa: monitorare le carenze più comuni per sensibilizzare le aziende e fornire indicazioni efficaci per risolverle	195
7.4.5.	Quinta tappa: superare la valutazione di profili di rischio teorici per arrivare ad una basata sulle situazioni reali	198

7.4.6.	Sesta tappa: consolidare il processo di <i>cyber risk management</i> in modo che diventi parte della cultura aziendale	199
7.5.	Il <i>cyber risk management</i> condiviso per un mercato assicurativo più efficiente	205
7.5.1.	Considerazioni finali	209
8.	I SINISTRI CYBER: PECULIARITÀ ED ESEMPI DI CASI REALI	
	<i>di Luca Ginocchietti</i>	
8.1.	Premessa	213
8.2.	Peculiarità della gestione sinistri <i>Cyber</i> rispetto ai sinistri tradizionali	213
8.3.	Il ruolo del <i>Loss Adjuster</i> nei sinistri <i>Cyber</i> ed il supporto in fase di <i>Incident Response</i>	215
8.4.	Caratteristiche Fondamentali dei Danni Coperti	216
8.5.	Caso Reale – <i>Ransomware</i>	223
8.6.	Conclusioni	225
9.	CONSIDERAZIONI SUL FUTURO DELL'ASSICURAZIONE CYBER	
	<i>di Massimiliano Rijllo</i>	
9.1.	Introduzione	231
9.2.	Tendenze emergenti nell'assicurazione <i>cyber</i>	231
9.3.	Il Mercato europeo: sfide e opportunità	234
9.4.	<i>Cyber insurtech</i>	236
9.5.	Riflessioni finali sulle tendenze	238
	BIBLIOGRAFIA E SITOGRADIA	239

Estratto

Estratto da un prodotto
in vendita su **ShopWKI**,
il negozio online di
Wolters Kluwer Italia

Vai alla scheda →

Wolters Kluwer opera nel mercato dell'editoria
professionale, del software, della formazione
e dei servizi con i marchi: IPSOA, CEDAM,
Altalex, UTET Giuridica, il fisco.

