

Inhaltsverzeichnis

Vorwort	V
Abkürzungsverzeichnis	XV
Grundlegendes Know-how	1
1 Wie ist eine „Cyberversicherung“ definiert?	1
2 Was versteht man unter „Silent Cyber Risk“?	3
3 Was versteht man unter dem Begriff Informationssicherheit?	5
4 Welche typischen Angriffsarten gibt es?	6
5 Wie hängen die Begriffe IT-Sicherheit, Datensicherheit und Datenschutz zusammen?	9
6 Was versteht man unter hybrider Kriegsführung	10
7 Ist die Cyberversicherung eine Konkurrenz für Cyber- Investitionen in einem Unternehmen?	10
8 Welche Begriffe sollte ein Vertriebsmitarbeiter verwenden/ verstehen?	12
9 Wie könnte eine geeignete Cyberversicherungssynopse aufgebaut sein?	14
10 Welche Fachbegriffe sollten Fachberater von Vermittlern beherrschen?	15
11 Welche Kommunikationsfallen sollte man vermeiden?	17
Sichtweisen und Positionen	19
12 Warum wird behauptet, dass die Cyberrisiko-Versicherung eine „große“ Zukunft hat?	19
13 Wie gut sind die unverbindlichen GDV-Musterbedingungen?	22
14 Welche Synopse ist die beste?	24
15 Wer sind die Stakeholder in einem Cyberrisiko- Transfer-Prozess?	26
16 Welche Mindestanforderungen müssen Unternehmen erfüllen, um versicherbar zu sein?	27

Inhaltsverzeichnis

17	Warum heißt es auch zum Thema Cyberversicherungen: Kleine Lügen, große Lügen und Statistiken?	28
Rechtliches Umfeld		31
18	Welche Informationen zu rechtlichen Regelungen/ Gesetzen sind im Internet verfügbar?	31
19	Was haben Versicherer bei der Einführung dieses neuen Produktes zu beachten?	32
20	Wie werden Prämieneinnahmen und Schadenzahlungen korrekt nach VAG gebucht?	33
21	Wie läuft das mit der Versicherung von Erpressungsgeldern?	34
22	Welche Haftungsnormen sind relevant?	36
23	Auf welchen rechtlichen Grundlagen fußt die IT-Sicherheit in Deutschland?	40
24	Wie relevant sind Obliegenheiten vor Eintritt des Versicherungsfalls (z.B. Stand der Technik)?	43
Risikohistorie und -entwicklung		45
25	Wie hat sich der Markt in Deutschland in der Vergangenheit entwickelt?	45
26	Wie werden sich Cyberrisiken und Cyberversicherungen in Zukunft entwickeln?	46
27	Wie entwickelt sich der Gesamtversicherungsmarkt in Bezug auf Silent Cyber 2.0?	51
28	Wie wird sich KI auf die Cyberversicherung auswirken? . .	52
29	Was geschieht mit sog. „unversicherbaren“ Risiken? . . .	53
Risikobetrachtungen		55
30	Welches sind die häufigsten Schäden?	55
31	Welche (technischen) Normen sind aus Sicht der Cyberversicherer relevant?	60
32	Wie könnte ein sinnvolles Statistiktool für Cyberversicherungen aussehen?	62
33	Was bringt die Integration präventiver Maßnahmen? . . .	63
34	Welche cyberrisiko-induzierten Schäden sind (Stand heute) nicht/kaum versicherbar?	65

35 Wie sieht eine typische Risikolandkarte eines Einzelhandelsunternehmens aus?	68
36 Welche Zertifizierungen geben Aufschluss über die Qualität der ITK-Sicherheit?	71
37 Was versteht man unter systemischen Cyber-Risiken?	72
38 Wie lassen sich Cyberrisiken von Unternehmen qualifizieren, quantifizieren und managen? (vgl. Frage 101 und Kumul Frage 103).....	73
39 Wie läuft ein typischer Ransomware-Schadenfall ab?	76
40 Wie entwickeln sich Cyber-Angriffs-Methoden und -Ziele?	77
Risikoquantifizierung	79
41 Wie findet man den richtigen ILF?.....	79
42 Inwieweit ist auch eine vertragliche Haftung versicherbar?	81
43 Wie errechnet sich eine bedarfsgerechte Prämie?.....	81
44 Welcher Fragebogen für welches Risiko?.....	86
45 Wie ermittle ich die korrekte Gesamt-Versicherungssumme?.....	88
46 Wie ermittle ich die richtige BU-Versicherungssumme?....	90
47 Wie ermittele ich die potentiellen Kosten von Cyber-Schadenfällen?.....	92
Schadenfall.....	95
48 Wie kann ein Dienstleister-/„Vendor“-Netzwerk aufgebaut sein?.....	95
49 Welche Obliegenheiten gibt es im Versicherungsfall?	96
50 Wie sollten sich Versicherte im Schadenfall verhalten?....	96
Versicherungsschutz	101
51 Sind Bußgelder versicherbar?	101
52 Welche Trigger (Versicherungsauslöser) finden in den Versicherungsbedingungen Anwendung?.....	103
53 Wie wirken Selbstbehalte bzw. Selbstbeteiligungen und Wartezeiten?.....	104
54 Wodurch wird der Versicherungsschutz einer Cyberversicherung ausgelöst?	105

55	Wie könnte eine Assistenz-/Krisenreaktionsdienstleistung in die Police integriert werden?.....	108
56	Wie wirkt eine Erprobungsklausel in Cyberversicherungen?	109
57	Wie verhält es sich mit der „Kriegsklausel“?.....	111
58	Welche Überschneidungen haben Cyberversicherungen mit herkömmlichen Versicherungen?	113
59	Was versteht man in der Cyberversicherung unter „reinen Vermögensschäden“?	117
60	Über welche Haupt-Versicherungsbestandteile verfügt eine Cyberversicherung?	118
61	Welche Deckungserweiterungen finden sich derzeit auf dem Markt?	119
62	Was bedeutet der Baustein PCI Bußgelder?.....	121
63	Wie funktioniert eine Kostenanrechnungsklausel in der Cyberversicherung?.....	122
64	Passen Vorrangigkeit und Regressmöglichkeit zusammen?.....	123
65	Inwieweit deckt eine Cyberversicherung Vorsatztaten?....	124
66	Warum bieten viele Versicherungskonzepte Versicherungsschutz für Aufwendungen vor Eintritt des Versicherungsfalls?.....	126
67	Welcher Versicherungsfallauslöser ist der beste?	127
68	Wieso werden Fake-President-Angriffe in Cyberversicherungen nicht als versichertes Cyberrisiko angesehen?	129
69	Was unterscheidet den Underwritingansatz der Cyberversicherung von dem der D&O?.....	130
70	Wie funktioniert die neue Kriegsklausel?	131
71	Wie wirkt sich die Höhe der Selbstbeteiligung auf die Meldeobligationen aus?	134
72	Wie funktioniert die „Zustimmung des Versicherers in Schriftform“?	135
73	Wie verhält sich die Cyberversicherung bei der Nutzung von Cloud Services? (siehe Frage 89).....	136

74	Was versteht man unter sog. Ransomware-Endorsements?	137
75	Wie wirken Territoriale Ausschlüsse?.....	139
Underwriting Grundlagen.....	143	
76	Warum unterscheidet man zwischen IT und OT?	143
77	Gibt es besonders gefährdete Branchen?	144
78	Welchen Grundwortschatz zur Cyberversicherung sollten Underwriter beherrschen?	147
79	Gibt es besondere Risikobranchen (vs. Geschäftsmodelle)?	148
80	Welche „Underwriting-Tools“ können sinnvollerweise genutzt werden?.....	149
81	Macht die Nutzung von „Cybersicherheits-Ratingagenturen“ Sinn?	152
82	Inwieweit sind ISO 27001 und KRITIS für das Cyber-Underwriting relevant?.....	155
83	Welche Haupt-Risikomerkmale/-aspekte sollte ein Cyber-Underwriter prüfen?.....	156
84	Was ist beim Underwriting-Aspekt „Region“ zu beachten? 159	
85	Was ist beim Underwriting-Aspekt „Zentralisierungsgrad“ zu beachten?.....	161
86	Was ist beim Underwriting-Aspekt „ITK-Abhängigkeit“ zu beachten?.....	162
87	Welche nicht auf die IT-Sicherheit gerichteten gesetzlichen Regelungen können aus Cyber-Underwriting-Sicht noch relevant sein?	163
88	Was ist beim Underwriting-Aspekt „Vernetzungsgrad“ zu beachten?.....	164
89	Was ist beim Underwriting-Aspekt „IT-Outsourcing-Grad“ zu beachten?	167
90	Was ist beim Underwriting-Aspekt „Organisations-/Formalisierungsgrad“ zu beachten?.....	169
91	Welche Fähigkeiten sollte ein Cyber-Underwriter (idealerweise) mitbringen	170
92	Wie bildet man Cyber-Underwriter aus?.....	171

Inhaltsverzeichnis

93	Welche Kumulrisiken existieren?	173
94	Welche Risikoinformationen müssen zur Risikobeurteilung erhoben werden?.....	175
95	Wie erhalte ich relevante Risikoinformationen über zu versichernde Unternehmen?.....	175
96	Wann machen Risikodialoge Sinn?.....	177
	Underwritingaspekte	179
97	Was ist im Zusammenhang mit Rückwärtsdeckungen zu beachten?.....	179
98	Was ist im Zusammenhang mit Vorwärtsdeckungen zu beachten?.....	180
99	Was versteht man unter Eigenhandel?	181
100	Was ist mit Blick auf Produkt- und Leistungsrisiken zu beachten?.....	183
101	Wie relevant ist die Unternehmensgröße für das Cyberrisiko eines Unternehmens?	185
102	Welche Besonderheiten sind bei der Versicherung von „contingent BI“ zu beachten?.....	187
103	Wie können Cyber-Kumulrisiken gemonitort werden? ...	189
104	Wo liegen – aus Cyber-Sicht – die Risikoschwerpunkte eines Produktionsbetriebs und eines Wohnungsunternehmens?	191
105	Welche Cyberrisiken herrschen bei Freiberuflern vor?....	193
106	Welche Risikofragen sind sinnvoll?	195
107	Was ist bei Versicherungsbeteiligungen zu beachten?	196
108	Was muss beim Ausfüllen von Fragebögen beachtet werden?	198
109	Wie wirken Sublimits und prozentuale Selbstbeteiligungen in gelayerten Versicherungsprogrammen?	201
	Internationale Aspekte.....	203
110	Harmoniert die DSGVO mit anderen internationalen Rechtsnormen (z.B. US Cloud-Act)?	203
111	Welche regionalen Risikounterschiede in der Cyberversicherung gibt es? Welche internationalen Unterschiede in der Gesetzgebung gibt es?	204

112 Welche Besonderheiten ergeben sich aus einem „Cyber-IVP“?	206
113 Was ist bei international agierenden Firmen/Online-Shops zu beachten?	207
114 Was ist bei der Festlegung des räumlichen Geltungsbereiches zu beachten?	209
115 Welches sind die führenden Märkte?	210
Weiterführende Informationen	213
116 Welche deutschen/europäischen Organisationen beschäftigen sich mit Informationssicherheit?	213
117 Welche Informationen zu aktuellen Cyber-Vorfällen sind im Internet frei verfügbar?	214
118 Welche Informationen zu Statistiken und Reports im Zusammenhang mit Cyberrisiken sind im Internet frei verfügbar?	215
119 Welche Schadenbeispiele gibt es?	216
120 Wo erhalte ich Informationen zu Versicherungslösungen?.	218
121 Wie gelange ich an zielgruppenbezogene Schadenbeispiele?	219
Abbildungsverzeichnis.....	221
Stichwortverzeichnis	225