

Inhaltsverzeichnis

Vorwort	V
1 Wie ist eine „Cyberversicherung“ definiert?	1
2 Was versteht man unter „Silent Cyber Risk“?	2
3 Warum unterscheidet man zwischen IT und OT?	3
4 Warum wird behauptet, dass die Cyberrisiko-Versicherung eine „große“ Zukunft hat?	4
5 Ist die Cyberversicherung eine Konkurrenz für Cyber-Investitionen in einem Unternehmen?	6
6 Welche typischen Angriffsarten gibt es?	7
7 Was versteht man unter dem Begriff Informationssicherheit?	9
8 Welche deutschen/europäischen Organisationen beschäftigen sich mit Informationssicherheit?	10
9 Welche Informationen zu rechtlichen Regelungen/Gesetzen sind im Internet verfügbar?	11
10 Welche Informationen zu aktuellen Cyber-Vorfällen sind im Internet frei verfügbar?	12
11 Welche Informationen zu Statistiken und Reports im Zusammenhang mit Cyberrisiken sind im Internet frei verfügbar?	13
12 Gibt es besonders gefährdete Branchen?	14
13 Welchen Grundwortschatz zur Cyberversicherung sollten Underwriter beherrschen?	15
14 Welche Begriffe sollte ein Vertriebsmitarbeiter verwenden/verstehen?	16
15 Was haben Versicherer bei der Einführung dieses neuen Produktes zu beachten?	18
16 Wie werden Prämieinnahmen und Schadenzahlungen korrekt nach VAG gebucht?	19
17 Harmoniert die DSGVO mit anderen internationalen Rechtsnormen (z.B. US Cloud-Act)?	20
18 Wie läuft das mit der Versicherung von Erpressungsgeldern?	21
19 Welche Haftungsnormen sind relevant?	22
20 Auf welchen rechtlichen Grundlagen fußt die IT-Sicherheit in Deutschland?	25
21 Sind Bußgelder versicherbar?	27

22	Welche regionalen Risikounterschiede in der Cyberversicherung gibt es? Welche internationalen Unterschiede in der Gesetzgebung gibt es?	29
23	Wie relevant sind Obliegenheiten vor Eintritt des Versicherungsfalls (z. B. Stand der Technik)?	30
24	Welche Trigger (Versicherungsauslöser) finden in den Versicherungsbedingungen Anwendung?	31
25	Wie wirken Selbstbehalte bzw. Selbstbeteiligungen und Wartezeiten?	32
26	Wodurch wird der Versicherungsschutz einer Cyberversicherung ausgelöst?	32
27	Wie kann ein Dienstleister-/„Vendor“-Netzwerk aufgebaut sein?	35
28	Wie könnte eine Assistenz-/Krisenreaktionsdienstleistung in die Police integriert werden?	35
29	Welches sind die häufigsten Schäden?	37
30	Welche Besonderheiten ergeben sich aus einem „Cyber-IVP“?	38
31	Welche Obliegenheiten gibt es im Versicherungsfall?	39
32	Wie wirkt eine Erprobungsklausel in Cyberversicherungen?	39
33	Was ist im Zusammenhang mit Rückwärtsdeckungen zu beachten?	40
34	Was ist im Zusammenhang mit Vorwärtsdeckungen zu beachten?	41
35	Welche (technischen) Normen sind aus Sicht der Cyberversicherer relevant?	42
36	Wie könnte ein sinnvolles Statistiktool für Cyberversicherungen aussehen?	44
37	Wie verhält es sich mit der „Kriegsklausel“?	45
38	Was versteht man unter Eigenhandel?	46
39	Welche Überschneidungen haben Cyberversicherungen mit herkömmlichen Versicherungen?	47
40	Wie könnte eine geeignete Cyberversicherungssynopse aufgebaut sein?	51
41	Was versteht man in der Cyberversicherung unter „reinen Vermögensschäden“?	52
42	Über welche Haupt-Versicherungsbestandteile verfügt eine Cyberversicherung?	52
43	Welche Deckungserweiterungen finden sich derzeit auf dem Markt?	53
44	Wie gut sind die unverbindlichen GDV-Musterbedingungen?	55
45	Was bedeutet der Baustein PCI Bußgelder?	56

46	Welche Synopse ist die beste?	57
47	Wie funktioniert eine Kostenanrechnungsklausel in der Cyberversicherung?	59
48	Passen Vorrangigkeit und Regressmöglichkeit zusammen?	60
49	Inwieweit deckt eine Cyberversicherung Vorsatztaten?	60
50	Warum bieten viele Versicherungskonzepte Versicherungsschutz für Aufwendungen vor Eintritt des Versicherungsfalls?	61
51	Welcher Versicherungsfallauslöser ist der beste?	62
52	Was ist mit Blick auf Produkt- und Leistungsrisiken zu beachten?	64
53	Wieso werden Fake-Präsident-Angriffe in Cyberversicherungen nicht als versichertes Cyberrisiko angesehen?	65
54	Was ist bei international agierenden Firmen/Online-Shops zu beachten? ..	66
55	Gibt es besondere Risikobranchen (vs. Geschäftsmodelle)?	68
56	Welche „Underwriting-Tools“ können sinnvoller Weise genutzt werden? ...	69
57	Macht die Nutzung von „Cybersicherheits-Ratingagenturen“ Sinn?	71
58	Wie relevant ist die Unternehmensgröße für das Cyberrisiko eines Unternehmens?	73
59	Inwieweit sind ISO 27001 und KRITIS für das Cyber-Underwriting relevant?	74
60	Welche Haupt-Risikomerkmale/-aspekte sollte ein Cyber-Underwriter prüfen?	75
61	Was ist beim Underwriting-Aspekt „Region“ zu beachten?	77
62	Was ist beim Underwriting-Aspekt „Zentralisierungsgrad“ zu beachten? ...	79
63	Was ist beim Underwriting-Aspekt „ITK-Abhängigkeit“ zu beachten?	80
64	Welche nicht auf die IT-Sicherheit gerichteten gesetzlichen Regelungen können aus Cyber-Underwriting-Sicht noch relevant sein?	80
65	Was ist beim Underwriting-Aspekt „Vernetzungsgrad“ zu beachten?	81
66	Was ist beim Underwriting-Aspekt „IT-Outsourcing-Grad“ zu beachten? ...	83
67	Was ist beim Underwriting-Aspekt „Organisations-/Formalisierungsgrad“ zu beachten?	85
68	Wie findet man den richtigen ILF?	86
69	Inwieweit ist auch eine vertragliche Haftung versicherbar?	87
70	Wie errechnet sich eine bedarfsgerechte Prämie?	88

71	Was bringt die Integration präventiver Maßnahmen?	91
72	Welche Fähigkeiten sollte ein Cyber-Underwriter (idealerweise) mitbringen	92
73	Wie bildet man Cyber-Underwriter aus?	93
74	Was ist bei der Festlegung des räumlichen Geltungsbereiches zu beachten?	94
75	Welche Besonderheiten sind bei der Versicherung von „contingent BI“ zu beachten?	95
76	Was unterscheidet den Underwritingansatz der Cyberversicherung von dem der D&O?	96
77	Welche cyberrisiko-induzierten Schäden sind (Stand heute) nicht/kaum versicherbar?	98
78	Welche Kumulrisiken existieren?	100
79	Wie können Cyber-Kumulrisiken gemonitort werden?	102
80	Welche Fachbegriffe sollten Fachberater von Vermittlern beherrschen? . .	103
81	Welche Kommunikationsfallen sollte man vermeiden?	104
82	Wer sind die Stakeholder in einem Cyberrisiko-Transfer-Prozess?	105
83	Wie werden sich Cyberrisiken und Cyberversicherungen in Zukunft entwickeln?	106
84	Welche Schadenbeispiele gibt es?	110
85	Wo erhalte ich Informationen zu Versicherungslösungen?	111
86	Wie gelange ich an zielgruppenbezogene Schadenbeispiele?	113
87	Welche Risikoinformationen müssen zur Risikobeurteilung erhoben werden?	113
88	Wie erhalte ich relevante Risikoinformationen über zu versichernde Unternehmen?	114
89	Wo liegen – aus Cyber-Sicht – die Risikoschwerpunkte eines Produktionsbetriebs und eines Wohnungsunternehmens?	115
90	Welche Cyberrisiken herrschen bei Freiberuflern vor?	117
91	Wie sieht eine typische Risikolandkarte eines Einzelhandelsunternehmens aus?	119
92	Welcher Fragebogen für welches Risiko?	121
93	Wie ermittle ich die korrekte Gesamt-Versicherungssumme?	123
94	Wie ermittle ich die richtige BU-Versicherungssumme?	124

95	Welche Risikofragen sind sinnvoll?	125
96	Wie ermittle ich die potentiellen Kosten von Cyber-Schadenfällen?	126
97	Welches sind die führenden Märkte?	128
98	Wie hat sich der Markt in Deutschland in der Vergangenheit entwickelt?	129
99	Wie hängen die Begriffe IT-Sicherheit, Datensicherheit und Datenschutz zusammen?	130
100	Welche Zertifizierungen geben Aufschluss über die Qualität der ITK-Sicherheit?	131
Abbildungsverzeichnis		133
Stichwortverzeichnis		137