

Inhalt

Vorwort	5
Abkürzungsverzeichnis	27
Einleitung	31
A. Problemstellung und Zielsetzung	31
I. Fortschreitende Digitalisierung	31
II. Einfallstor für Cyberkriminalität	31
III. Risikominimierung und -transfer	34
B. Gang der Arbeit	36
Kapitel 1: Cyberrisiken	39
A. Cyberrisiken im Allgemeinen	39
I. Anknüpfungspunkt: Verwendung von IT	39
II. Hinter der Verwirklichung der Risiken stehende Ursachen	40
B. Angriffsszenarien	40
I. Data Breach	41
II. Schadprogramme	43
III. Denial of Service-Attacke	45
IV. CEO Fraud	46
V. Phishing	47
C. Auswirkungen	48
I. Eigenschäden	49
II. Drittschäden	50
D. Umgang mit Cyberrisiken	51
I. Cyberrisiken und Strafrecht	51
II. Gesetzgeberische Bestrebungen zur Schaffung von IT-Sicherheit	52
III. Cyberrisiken und Versicherungsschutz	54

Kapitel 2: Die spezielle Cyberversicherung	57
A. Einführung in die Cyberversicherung	57
I. Definition der Cyberversicherung	57
II. Marktentwicklung	58
III. Untersuchungsgegenstand	60
B. Versicherungsumfang nach den AVB Cyber von 2017	61
I. Allgemeines zu den AVB	61
II. Versichertes Risiko in der Cyberversicherung	68
III. Versicherungsfall	102
IV. Einschränkungen und Ausschlüsse des Versicherungsschutzes ..	111
V. Deckungsbausteine der AVB Cyber	177
C. Zusammenfassung und Bewertung	221
Kapitel 3: Absicherung von Cyberrisiken durch traditionelle Versicherungen	225
A. IT-Klauseln in Unternehmensversicherungen	225
I. Sachversicherungen	225
II. Haftpflichtversicherungen	235
III. Zusatzbaustein Cyber-Assistance	250
B. Silent Cyber	257
I. Einführung in die Problematik	257
II. Mit „non affirmative“ Risiken verbundene Herausforderungen ..	258
III. „Non-affirmative“ Risiken in traditionellen gewerblichen Versicherungen	264
IV. Bewertung der Problematik	279
C. Zusammenfassung	283
Kapitel 4: Verhältnis zwischen einzelnen Versicherungen	285
A. Mehrfachversicherung, § 78 VVG	285
I. Rechtsfolgen im Außenverhältnis	287
II. Rechtsfolgen im Innenverhältnis	287

Inhalt	9
B. Subsidiaritäts- und Vorrangigkeitsklauseln	288
I. Subsidiaritätsklauseln	288
II. Vorrangigkeitsklausel, A1-12 AVB Cyber	289
C. Zusammenfassung	296
Schlussstein	299
A. Risikominimierung	299
B. Risikotransfer	300
C. Resümee	301
Literaturverzeichnis	305

Inhaltsverzeichnis

Vorwort	5
Abkürzungsverzeichnis	27
Einleitung	31
A. Problemstellung und Zielsetzung	31
I. Fortschreitende Digitalisierung	31
II. Einfallstor für Cyberkriminalität	31
1. Cybervorfälle	33
2. Motivation der Täter	34
III. Risikominimierung und -transfer	34
B. Gang der Arbeit	36
Kapitel 1: Cyberrisiken	39
A. Cyberrisiken im Allgemeinen	39
I. Anknüpfungspunkt: Verwendung von IT	39
II. Hinter der Verwirklichung der Risiken stehende Ursachen	40
B. Angriffsszenarien	40
I. Data Breach	41
II. Schadprogramme	43
III. Denial of Service-Attacke	45
IV. CEO Fraud	46
V. Phishing	47
C. Auswirkungen	48
I. Eigenschäden	49
II. Drittschäden	50
D. Umgang mit Cyberrisiken	51
I. Cyberrisiken und Strafrecht	51

II. Gesetzgeberische Bestrebungen zur Schaffung von IT-Sicherheit	52
III. Cyberrisiken und Versicherungsschutz	54
1. Versicherbarkeit von Cyberrisiken	55
2. Spezielle Cyber-Versicherungen	55
3. Traditionelle Versicherungspolicen	56
Kapitel 2: Die spezielle Cyberversicherung	57
A. Einführung in die Cyberversicherung	57
I. Definition der Cyberversicherung	57
II. Marktentwicklung	58
1. Der deutsche Cyberversicherungsmarkt	58
2. Zahlen und Fakten	59
III. Untersuchungsgegenstand	60
B. Versicherungsumfang nach den AVB Cyber von 2017	61
I. Allgemeines zu den AVB	61
1. Aufbau der Musterbedingungen	62
2. Auslegung von AVB	63
a. Auslegungsmaßstab	63
b. Verkehrskreisbezogene Auslegung	64
c. Grenzen der Auslegung	64
aa) Kontrollfreiheit des Vertragskerns	65
bb) Abstellen auf das Verständnis eines IT-Fachmannes	66
cc) Stellungnahme	67
II. Versichertes Risiko in der Cyberversicherung	68
1. Informationssicherheitsverletzung	68
a. Schutzgut	68
aa) Elektronische Daten des Versicherungsnehmers	69
(1) Speicherform	69
(2) Inhaberschaft der Daten	69
(a) „Dateneigentum“	70
(b) Zuweisung des Datenrechts	71
(aa) Inhaber des Datenträgers	71

(bb) Erzeugung der elektronischen Daten .	71
(cc) Möglichkeit der Einwirkung auf die Daten	72
(dd) Stellungnahme	72
bb) Informationsverarbeitende Systeme	73
(1) Auslegung des Begriffs	73
(2) Inanspruchnahme externer Dienstleistungen	74
(a) Outsourcing	74
(b) Ausschluss bei Verfügbarkeitsbeeinträchtigungen	75
(c) Wirksamkeit des Ausschlusses	75
(aa) § 305c Abs. 1 BGB	75
(bb) § 307 Abs. 1 S. 1 i.V.m. Abs. 2 BGB	76
(cc) § 307 Abs. 1 S. 2 BGB	77
(d) Reichweite des Ausschlusses	78
cc) Nutzung zur Ausübung der betrieblichen oder beruflichen Tätigkeit	79
b. Schutzziele	80
aa) Verfügbarkeit	81
bb) Integrität	81
cc) Vertraulichkeit	82
c. Auslösendes Ereignis der Informationssicherheitsverletzung	82
aa) Versicherte Ereignisse	83
(1) Angriff auf Daten oder Systeme	83
(2) Unberechtigter Zugriff auf elektronische Daten .	84
(3) Eingriff in informationsverarbeitende Systeme ...	84
(a) Begriffsbestimmung	85
(aa) Der Eingriff als beherrschbares Verhalten	85
(bb) Der Eingriff als unerwünschtes Verhalten	85
(b) Konkrete Eingriffsbeispiele	87
(c) Abgrenzung zu einem Angriff	89

(4) Verletzung von datenschutzrechtlichen Vorschriften durch den Versicherungsnehmer ...	89
(a) Datenschutzrechtliche Vorschriften	89
(b) Verantwortlicher	90
(c) Verletzung durch Unterlassen	91
(5) Schadprogramme	92
bb) Systeme „des Versicherungsnehmers“	93
(1) Bedeutung bei Inanspruchnahme externer Dienstleistungen	93
(2) Im (Home-)Office genutzte, private Geräte	94
2. Vermögensschaden	95
a. Abgrenzung zu Sachschäden	95
b. Mittelbare Vermögensschäden	95
aa) Abgeleitete Vermögensschäden, die auf dem Abhandenkommen des Datenträgers beruhen	96
bb) Abgeleitete Vermögensschäden, die auf der Beschädigung des Datenträgers beruhen	97
3. Übertragung der Erkenntnisse auf die Angriffsszenarien	98
a. Data Breach	98
b. DoS-Attacke	99
c. Schadprogramme	99
d. CEO-Fraud	100
e. Phishing	100
4. Schlussfolgerungen	101
III. Versicherungsfall	102
1. Manifestationsprinzip	102
a. Problematik: Feststellung der Informationssicher- heitsverletzung	102
b. Meinungsstand	103
c. Stellungnahme	103
2. Beweislast für das Vorliegen des Versicherungsfalls	104
3. Versicherter Zeitraum	105
a. Nachdeckung	105

aa) Notwendigkeit der Nachhaftungsregelung	105
bb) Gründe für die Vertragsbeendigung	106
(1) Benannte Beendigungsgründe	106
(2) Erweiterung der Nachdeckung auf den Widerruf (§ 8 Abs. 1 VVG)	106
(a) Der Widerruf nach § 8 Abs. 1 VVG und seine Folgen	106
(b) Stellungnahme	108
b. Rückwärtsdeckung	109
aa) Notwendigkeit der Rückwärtsdeckung	109
bb) Voraussetzungen für die Rückwärtsdeckung nach A1-6 AVB Cyber	109
cc) Verhältnis zu § 2 Abs. 2 S. 1 VVG	110
4. Schlussfolgerungen	110
IV. Einschränkungen und Ausschlüsse des Versicherungsschutzes .	111
1. Obliegenheiten	111
a. Obliegenheiten vor Eintritt des Versicherungsfalls	112
aa) Gesetzliche Obliegenheiten	112
(1) Vorvertragliche Anzeigepflicht, § 19 VVG	113
(a) Sinn und Zweck	113
(b) Relevanz bei Cyberrisiko-Versicherung	113
(aa) Musterfragebogen des GDV zur Risikoerfassung	114
(bb) Risikokategorien	115
(c) Rechtsfolgen bei Verletzung der Anzeigeobliegenheiten	115
(aa) Verwirkung der Rechte durch Versicherer	116
(bb) Nach dem Verschulden abgestuftes Sanktionssystem	116
(2) Gefahrerhöhung, §§ 23 – 27 VVG	117
(a) Begriff der Gefahrerhöhung	118
(b) Cyberrelevante Gefahrerhöhungen	119
(aa) Steigende Zahl an Cyberangriffen	119

(bb) Nutzung von nicht länger unterstützter Software	119
(cc) Zunehmende Homeoffice-Tätigkeiten	120
(c) Rechtsfolgen	122
(aa) Kündigung	122
(bb) Prämien erhöhung	123
(cc) Leistungsfreiheit	123
bb) Vertragliche Obliegenheiten	125
(1) Gewährleistung der IT-Sicherheit	125
(a) Datensicherung	126
(aa) Inhalt der Obliegenheit	126
(bb) Turnus der Datensicherung	127
(b) Zugangssicherung	128
(aa) Komplexität eines Passworts	129
(bb) Geräte mit erhöhtem Risiko	129
(c) Schutz gegen Schadsoftware	132
(d) Sicherheitsupdates	132
(aa) Notwendigkeit der Vornahme von Sicherheitsupdates	133
(bb) Verkehrskreisbezogene Kenntnis	133
(e) Technikstandard in Cyberversicherungspolicen	134
(aa) „Stand der Technik“	135
(bb) Verstoß gegen das Transparenzgebot	136
(cc) Zu gewährendes Schutzniveau im versicherten Unternehmen	137
(2) Einhaltung von Sicherheitsvorschriften	139
(a) Gesetzliche Sicherheitsvorschriften	139
(aa) Auf die Gewährleistung der IT-Sicherheit abzielende Vorschriften	139
(bb) Datenschutzrechtliche Vorschriften	140
(b) Behördliche Sicherheitsvorschriften	141
(c) Vertragliche Sicherheitsvorschriften	142

(d) Wirksamkeit der Klausel	142
(aa) Verstoß gegen das Transparenzgebot	142
(bb) Stellungnahme	143
(3) Beseitigung von gefahrdrohenden Umständen auf Verlangen des Versicherers	144
(4) Rechtsfolgen bei Obliegenheitsverletzung	145
(a) Kündigung	145
(b) Leistungsfreiheit	146
(aa) Vertraglich vereinbarte Leis- tungsfreiheit	146
(bb) Beweislastverteilung	146
b. Obliegenheiten bei und nach Eintritt des Versiche- rungsfalles	147
aa) Gesetzliche Obliegenheiten nach § 82 VVG	147
(1) § 82 Abs. 1 VVG	147
(2) § 82 Abs. 2 VVG	148
(3) Rechtsfolge	149
bb) Vertragliche Obliegenheiten	149
(1) Anzeigepflicht	149
(2) Auskunftspflicht	150
(3) Sonstige vertragliche Obliegenheiten	150
(4) Rechtsfolge	151
(a) Leistungsfreiheit	151
(b) Erforderlicher Hinweis durch Versicherer ..	151
c. Zurechnung des Verhaltens Dritter	152
aa) Allgemeines	152
bb) Repräsentantenhaftung	153
cc) Repräsentanten im Sinne von A1-9 AVB Cyber	154
dd) Herausforderung beim Einsatz externer IT- Dienstleister	154
2. Risikoausschlüsse	156
a. Krieg, Terror, politische Gefahren	157
aa) Krieg	157

(1) "NotPeyta" als kriegerischer Akt	157
(2) Kriegsbegriff	158
(a) Allgemeine versicherungsrechtliche Deutung	158
(b) Auslegung der Klausel A1-17.2 AVB Cyber	160
(3) Schlussfolgerungen	160
bb) Terror	161
cc) Politische Gefahren	162
b. Lösegeldforderungen	163
aa) Möglichkeit der Absicherung von Lösegeldfor- derungen	163
bb) Umsetzung in der Praxis	164
c. Absicherung von Bußgeldern	164
aa) Abweichende Regelung in Vertragswerken	164
(1) Rechtliche Zulässigkeit	165
(a) Verstoß gegen ein Verbotsgebot im Sinne von § 134 BGB	165
(b) Sittenwidrigkeit nach § 138 BGB	166
(2) Weitere Wirksamkeitsbedenken	167
bb) Fazit	168
d. Vorsatz und wissentliche Pflichtverletzungen	168
aa) Allgemeines	168
bb) Regelungsgehalt	169
cc) Unterlassen von notwendigen Sicherheitsmaß- nahmen	170
(1) Herbeiführung des Versicherungsfalls durch Unterlassen, § 81 VVG	170
(2) Grob fahrlässige Herbeiführung des Ver- sicherungsfalles, § 81 Abs. 2 VVG	171
(3) Beweislastverteilung	172
e. Cyberangriffe auf Fahrzeuge	173
f. Ausfall Infrastruktur	174
aa) Allgemeines	174

bb) Wirksamkeit des Risikoausschlusses	175
(1) Ausfälle von Gebietskörperschaften und Infrastrukturbetrieben	175
(2) Betroffenheit von dem Ausfall	176
(3) Fazit	177
V. Deckungsbausteine der AVB Cyber	177
1. Service-/Kostenbaustein (A2)	178
a. Aufwendungen vor Eintritt des Versicherungsfalles	178
aa) Unmittelbar bevorstehender Schaden	178
bb) Erforderliche Maßnahmen	179
cc) Anzeigebliegenheit	180
(1) Sinn und Zweck	180
(2) Über die Anzeige hinausgehender Abstimmungsvorbehalt	180
dd) Verhältnis zu § 83 VVG und § 90 VVG	181
b. Kostenpositionen nach Eintritt des Versicherungsfalles ..	182
aa) Ermittlungs-/Schadensfeststellungskosten	182
bb) Benachrichtigungskosten	183
cc) Call-Center-Kosten	183
dd) Kosten für weiteres Krisenmanagement	184
ee) Abstimmungs-/Zustimmungsvorbehalte	184
c. Schlussfolgerungen	185
2. Drittschadenbaustein (A3)	186
a. Haftungsszenarien	186
aa) Aus Vertragsverhältnis	187
(1) Pflichtverletzungen	188
(a) Nicht (vertragsgemäß)e Leistung	188
(b) Verletzung von Sorgfaltspflichten	189
(c) Verletzung von Informationspflichten	190
(d) Verletzung von vertraglichen Geheimhaltungspflichten	191
(e) Vorvertragliche Pflichtverletzung	191
(2) Vertretenmüssen	192

(a) Beweislast	192
(b) Standardisierte Haftungsbeschränkungen .	193
(c) Zurechnung des Verhaltens eines Drittens	193
(3) Schaden	193
bb) Deliktische Ansprüche	194
(1) Verkehrssicherungspflicht	194
(2) Haftungsgrundlagen	195
(a) Art. 82 DSGVO	196
(aa) Verstoß gegen die DSGVO	196
(bb) Pflichtiger	196
(cc) Verschuldensunabhängige Haf- tung und Exkulpationsmöglichkeit ..	197
(dd) Erstattungsfähiger Schaden	197
(b) § 69 Abs. 1 S. 1, S. 4 TKG	198
(c) § 1 Abs. 1 S. 1 ProduktHaftG	198
(d) § 823 Abs. 1 BGB	199
(aa) Produkthaftung	199
(bb) Weitere Haftungsszenarien	200
(e) § 823 Abs. 2 BGB i.V.m. einem Schutzgesetz	201
b. Übernahme durch den Versicherer	202
aa) Vorliegen eines Vermögensschadens	203
(1) Persönlichkeitsrechtsverletzungen	203
(2) Deckungserweiterung in A3-4.1 AVB Cyber	204
bb) Vertragliche Haftungsansprüche	205
(1) Auf Vertragserfüllung beruhende Ansprüche ...	205
(2) Ansprüche außerhalb der gesetzlichen Haftpflicht	205
c. Inanspruchnahme durch einen Dritten	206
aa) Ansprüche mitversicherter Unternehmen	206
bb) Geltendmachung durch qualifizierte Einrich- tung im Musterfeststellungsverfahren	207
(1) Die Musterfeststellungsklage	207

(2) Qualifizierte Einrichtung als Dritter	208
d. Schlussfolgerungen	209
3. Eigenschadenbaustein (A4)	210
a. Betriebsunterbrechung	210
aa) Unterbrechungsschaden	211
(1) Berechnung der Entschädigung	212
(2) Dauer der Entschädigung	212
bb) Ausgeschlossene Unterbrechungsschäden	213
(1) Beabsichtigte Maßnahmen	214
(2) Einsatz neuer IT-Systeme, Verfahren oder Software	214
(3) Einsatz ungetesteter IT-Systeme, Verfahren oder Software	216
(4) Einsatz unlizenziert IT-Systeme, Verfahren oder Software	216
(5) Softwarefehler	217
b. Wiederherstellung von Daten	218
aa) Versicherte Daten	218
bb) Notwendige Aufwendungen und Notwendigkeit der Datenwiederherstellung und Schadprogrammentfernung	219
(1) Notwendige Aufwendungen	219
(2) Notwendigkeit der Datenwiederherstellung	219
cc) Risikoausschlüsse	220
c. Schlussfolgerungen	220
C. Zusammenfassung und Bewertung	221
Kapitel 3: Absicherung von Cyberrisiken durch traditionelle Versicherungen	225
A. IT-Klauseln in Unternehmensversicherungen	225
I. Sachversicherungen	225

1.	Klassische Elektronikversicherung	226
a.	Beeinträchtigung von Daten	226
b.	Obliegenheiten des Versicherungsnehmers	227
c.	Überschneidung mit dem Deckungsschutz der Cyberversicherung	228
2.	Klauseln Datenversicherung	228
a.	Versicherte Gefahren	229
aa)	Gefahren in den IT-Systemen des Versicherungsnehmers	229
bb)	Gefahren in den IT-Systemen eines externen IT-Dienstleisters	230
cc)	Klauseln „erweiterte Datenversicherung“	230
dd)	Klauseln Softwareversicherung	231
b.	Entschädigungsleistung	232
c.	Überschneidung mit dem Deckungsschutz der Cyberversicherung	232
3.	Klauseln Mehrkostenversicherung	233
a.	Entschädigungsleistung	234
b.	Überschneidung mit dem Deckungsschutz der Cyberversicherung	234
II.	Haftpflichtversicherungen	235
1.	„Klassische“ Haftpflichtversicherung	235
2.	Betriebshaftpflichtversicherung	236
a.	Übernahme von IT-Risiken	236
aa)	Versicherte Risiken	236
(1)	Datenveränderungen bei Dritten	236
(2)	Störungen des Zugangs Dritter zum elektronischen Datenaustausch	238
(3)	Verletzung von Persönlichkeitsrechten	238
bb)	Nicht versicherte Risiken	239
(1)	Ausschluss für IT-spezifische Leistungen	239
(2)	Weitere Risikoausschlüsse	239
b.	Obliegenheiten	240

c. Überschneidung mit dem Deckungsschutz der Cyberversicherung	241
3. Haftpflichtversicherung für IT-Dienstleister (BBR-ITD)	242
a. Versicherte Tätigkeiten	243
b. Versicherte Datenschäden	243
aa) Software/Hardwarebezogene Tätigkeiten	243
(1) Versicherte Schäden	243
(2) Vorkehrungen zur Gewährleistung der Sicherheit der Daten	244
(a) Verhüllte Obliegenheit	245
(b) Auslegung der Klausel	245
(c) Rechtsfolge der Qualifizierung der Klauseln als verhüllte Obliegenheiten	246
(aa) Unwirksamkeit wegen Verstoß gegen § 307 Abs. 1 S. 2 BGB	246
(bb) Differenzierte Betrachtung	247
(cc) Stellungnahme	247
(bb) Providertätigkeiten	248
(cc) Zwischenfazit	249
c. Überschneidungen mit dem Deckungsschutz der Cyberversicherung	250
III. Zusatzbaustein Cyber-Assistance	250
1. Bedeutung von Assistance-Leistungen für Unternehmen	251
2. Assistance-Leistungen des Cyber-Assistance-Bausteins	252
a. Assistance im Falle von Cybermobbing	252
b. Assistance im Falle des Identitätsmissbrauchs	253
aa) Versichertes Risiko: Identitätsmissbrauch	253
(bb) Identitätsmissbrauch im Unternehmen	254
(cc) Ausgestaltung der Unterstützung	254
c. Assistance im Falle des Datenverlustes	255
aa) Versichertes Risiko: Datenverlust	255
(bb) Versicherte Daten	256
B. Silent Cyber	257

I.	Einführung in die Problematik	257
II.	Mit „non affirmative“ Risiken verbundene Herausforderungen	258
1.	Deckung eines nicht einkalkulierten Schadens	258
2.	Fehlende Transparenz	259
a.	Unsicherheit auf Seiten der Versicherer und Versicherungsvermittler	259
b.	Gefahr für den Versicherungsnehmer	259
3.	Bindung an den geschlossenen Vertrag	260
a.	Anspruch auf Vertragsanpassung	261
b.	Kündigungsmöglichkeit des Versicherers	261
aa)	Kündigung nach Eintritt des Versicherungsfalles	261
bb)	Kündigung von Versicherungsverträgen nach § 11 VVG	262
c.	Leistungspflicht des Versicherers im Versicherungsfall	263
III.	„Non-affirmative“ Risiken in traditionellen gewerblichen Versicherungen	264
1.	Technische Versicherungen	264
a.	Allgefahrenversicherungen	264
aa)	Elektronikversicherung	264
bb)	Maschinenversicherung	265
b.	Cyberrisiko als Ursache für einen Sachschaden	266
2.	Feuerversicherung	267
a.	Benannte Gefahren	267
b.	Versicherte Schäden	268
aa)	Schäden an Betriebsstätten	268
bb)	Betriebsunterbrechungsschäden	268
c.	Obliegenheit zur Anzeige von Gefahrerhöhungen, § 23 Abs. 3 VVG	269
3.	D&O-Versicherung zur Absicherung der Unternehmensleitung	270
a.	Versicherungskonzept der D&O-Versicherung	270
b.	Cybersicherheit als Teil der unternehmerischen Lei- tungsverantwortung	271

aa)	Vornahme von Maßnahmen zur Gewährleistung der IT-Sicherheit	271
(1)	Die Business Judgment Rule	271
(2)	Die Verantwortlichkeit der Geschäftsleitung	273
bb)	Absicherung des Risikos durch eine Versicherungslösung	274
c.)	Versicherte Vermögensschäden	275
d.)	Drohende Zweckentfremdung der D&O-Versicherung? .	276
4.)	Vertrauensschadenversicherung	276
a.)	Versicherungskonzept der Vertrauensschadenversicherung	276
b.)	Versicherungsschutz für vorsätzliche unerlaubte Handlungen	277
c.)	Ersatz von Vermögensschäden	279
IV.)	Bewertung der Problematik	279
1.)	Erkenntnisse der BaFin	279
2.)	Lösungsansatz	280
a.)	Gezielte Absicherung von Cyberrisiken durch traditionelle Produkte	281
b.)	Risikoausschluss für Cyberrisiken	282
C.)	Zusammenfassung	283
Kapitel 4: Verhältnis zwischen einzelnen Versicherungen		285
A.)	Mehrfachversicherung, § 78 VVG	285
I.)	Rechtsfolgen im Außenverhältnis	287
II.)	Rechtsfolgen im Innenverhältnis	287
B.)	Subsidiaritäts- und Vorrangigkeitsklauseln	288
I.)	Subsidiaritätsklauseln	288
II.)	Vorrangigkeitsklausel, A1-12 AVB Cyber	289
1.)	Gründe für die vorrangige Leistungspflicht des Cyberversicherers	289
2.)	Regelungsgehalt der Vorrangigkeitsklausel	290
a.)	Rechtsfolgen im Außenverhältnis	290

aa) Abbedingung der Wahlmöglichkeit nach § 78 Abs. 1 VVG	290
bb) Stellungnahme	291
b. Rechtsfolgen im Innenverhältnis	292
aa) Abbedingung des Gesamtschuldnerausgleichs nach § 78 Abs. 2 S. 1 VVG	292
bb) Meinungsstand	293
cc) Kritische Analyse	293
dd) Stellungnahme	295
ee) Zwischenergebnis	296
C. Zusammenfassung	296
 Schlussstein	299
A. Risikominimierung	299
B. Risikotransfer	300
C. Resümee	301
 Literaturverzeichnis	305