

# Rechtshandbuch Cyber-Security

IT-Sicherheit, Datenschutz, Gesellschaftsrecht,  
Compliance, M&A, Versicherungen,  
Aufsichtsrecht, Arbeitsrecht, Litigation

Herausgegeben von

**Dr. Detlev Gabel**

Rechtsanwalt, Frankfurt am Main

**Dr. Tobias A. Heinrich, LL.M. (London)**

Rechtsanwalt, Frankfurt am Main

und

**Dr. Alexander Kiefner**

Rechtsanwalt, Frankfurt am Main

Bearbeitet von

Steven Chabinsky; Melody Chan; Denise Cheung; Dr. Detlev Gabel;  
Tobias Gans; Dr. Tobias A. Heinrich, LL.M. (London); Dr. Justus  
Herrlinger; Dr. Alexander Kiefner; Markus Langen, LL.M. (Sydney);  
Aurora Leung; David Markoff; Robert Mechler; Dr. Lars Ole Petersen;  
F. Paul Pittman; Prof. Dr. Igor Podebrad; Hendrik Röger; Dr. Dominik  
Stier; Douglas Tan; John Timmons; Dr. Philip Trillmich; Dr. Andreas  
Wieland; Mark Williams; Prof. Dr. Norbert Wimmer; Christian  
Wirth; Karl-Jörg Xylander

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

**Bibliografische Information der Deutschen Nationalbibliothek**

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.de> abrufbar.

ISBN 978-3-8005-0012-3

**dfv** Mediengruppe

© 2019 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft,  
Frankfurt am Main

[www.ruw.de](http://www.ruw.de)

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Satzkonvertierung: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

Druck und Verarbeitung: WIRMACHENDRUCK GmbH, 71522 Backnang

Printed in Germany

# Inhaltsverzeichnis

Vorwort .....	V
Abkürzungsverzeichnis und Verzeichnis der abgekürzt zitierten Literatur .....	XXVII

## Kapitel 1 Einleitung

*Prof. Dr. Igor Podebrad/Dr. Detlev Gabel*

<b>I. Top-Thema „Cyber-Security“</b> .....	1
<b>II. Gängige Formen von Cyber-Attacken</b> .....	4
1. Erpressung durch Computersabotage – Ransomware .....	4
2. Computersabotage um der Sabotage willen – Malware .....	4
3. Überlastung von Infrastrukturen – DDoS-Attacken .....	5
4. Gezielter dauerhafter Zugriff auf IT-Systeme – Advanced Persistent Threat (APT-Angriff) .....	5
5. Die Chef-Masche – CEO-Fraud .....	6
<b>III. Kosten</b> .....	6
<b>IV. Vorbeugende Maßnahmen („Preparedness“)</b> .....	7
1. Der strategische Rahmen .....	8
2. Praktische Maßnahmen .....	9
a) Bestimmung der „Cyber-Sicherheits-Exposition“ durch das Management .....	10
b) Ein kritischer Blick seitens des Risikomanagements .....	10
c) Umsetzung geeigneter Maßnahmen durch den CIO und den CISO .....	11
<b>V. Verhalten im Ernstfall („Response“)</b> .....	12
1. Erfassung und Bewertung des Angriffs („Identification“) .....	12
2. Schadensbegrenzung („Minimization“) .....	12
3. Dokumentation aller relevanten Informationen („Documentation“) .....	13
4. Benachrichtigung Dritter („Notification“) .....	13
5. Rückkehr zum Normalbetrieb („Remediation“) .....	13
<b>VI. Querschnittsthema Cyber-Security</b> .....	13

VII

**Kapitel 2**  
**Gesellschaftsrecht**  
**(Unternehmensleitung und Unternehmensorganisation)**

*Dr. Alexander Kiefner*

<b>I. Rechtsgrundlagen</b> .....	17
1. Einleitung .....	17
2. Cyber-Security, Compliance und Risikomanagement .....	18
3. Rechtsgrundlagen .....	19
<b>II. Kollisionsrecht und Verhältnis zu ausländischen Rechtsquellen.</b>	21
<b>III. Preparedness</b> .....	22
1. Cyber-Security bezogene Risikovorsorge und Compliance als Rechtspflicht der Unternehmensleitung .....	22
2. Risikoanalyse .....	24
a) Analyse und Ordnungsrahmen .....	25
b) Umfang der Analyse .....	26
c) Risikokategorisierung und Risikobewertung .....	28
d) Ständige Aktualisierung der Risikoanalyse und -bewertung ..	29
3. Einführung einer der Analyse und Bewertung entsprechenden Cyber-Security-Governance .....	30
a) Möglichkeiten der Risikobehandlung .....	30
b) Umsetzung durch Cyber-Security-Programm .....	32
c) Preparedness auf dem Prüfstand .....	34
4. Praktische Notwendigkeiten und Folgen für die Gremienarbeit und -organisation .....	35
a) Das richtige „Mindset“ auf Ebene der Unternehmensleitung .....	35
b) Das „richtige“ Know-how auf Ebene von Vorstand und Aufsichtsrat .....	36
c) Organisatorische Umsetzungsmaßnahmen .....	38
d) Risikoexternalisierung durch Versicherungslösungen .....	41
<b>IV. Response</b> .....	43
1. Organisationsvorkehrungen für den Ernstfall .....	43
a) Cyber Incident Response Plan (CIRP) .....	43
b) Das Response-Team .....	45
c) Bedeutung einer effektiven IT-Forensik nach Cyber-Angriff .....	47
2. Business Judgment Rule und Response .....	48

3. Insiderrecht und Ad-hoc-Publizität .....	50
4. Nachgelagerte Maßnahmen nach einer Cyber-Attacke (mittelfristige Reaktion) .....	55
<b>V. Haftungsrisiken für die Unternehmensleitung .....</b>	<b>56</b>
1. Innenhaftung wegen fehlender oder unzureichender Preparedness .....	56
2. Innenhaftung wegen fehlender oder unzureichender Response .....	57
3. Mögliche ersatzfähige Schäden .....	58
4. Überwälzung von Unternehmensbußgeldern auf Geschäftsleiter .....	59

### **Kapitel 3 Mergers & Acquisitions**

*Dr. Tobias A. Heinrich, LL.M. (London)*

<b>I. Einführung .....</b>	<b>62</b>
<b>II. Fallbeispiele .....</b>	<b>63</b>
1. Verizon/Yahoo .....	63
2. FedEx/TNT .....	64
3. Marriott/Starwood .....	64
<b>III. Preparedness .....</b>	<b>65</b>
1. Bedeutung und Gegenstand der Cyber-Due Diligence .....	65
2. Eckpunkte der Cyber-Due Diligence .....	67
3. Durchführung einer Cyber-Due Diligence .....	68
a) Operative Risikoanalyse und Verortung digitaler Assets .....	68
b) Compliance-Risikoanalyse .....	69
c) Risikomanagementsysteme und Compliance .....	69
d) Spezialgesetzliche Regelungen .....	70
e) Datenschutz .....	71
f) Individuelles Handeln als Risikofaktor .....	71
g) Outsourcing an Dritte .....	72
h) Cyber-Versicherungen .....	73
i) Meldepflichten .....	73
j) Cyber-Security-Governance .....	74
k) Stellenwert auf Ebene der Unternehmensleitung .....	75
l) Vorbereitende Maßnahmen für den Ernstfall .....	76
m) Betroffene Länder .....	77

Inhaltsverzeichnis

<b>IV. Response</b> .....	78
1. Vertragliche Instrumente zur Absicherung von Cyber-Risiken ...	78
a) Kaufpreisanpassung .....	80
b) Selbstständige Garantien .....	80
c) Freistellungen .....	83
d) MAC-Klauseln .....	84
e) W&I-Versicherungen .....	85
2. Integrationsplanung .....	86

**Kapitel 4**  
**Datenschutz**

*Dr. Detlev Gabel*

<b>I. Datenschutzrechtliche Grundlagen</b> .....	88
1. Cyber-Security und Datenschutzrecht .....	88
2. DSGVO .....	89
3. BDSG (neu) .....	91
4. ePrivacy-Verordnung (Entwurf) .....	91
<b>II. Kollisionsrecht</b> .....	92
<b>III. Preparedness</b> .....	94
1. DSGVO .....	94
a) Grundsatz der Integrität und Vertraulichkeit .....	94
b) Sicherheit der Verarbeitung von personenbezogenen Daten ..	95
c) Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen .....	99
d) Datenschutz-Folgenabschätzung .....	101
e) Einsatz von Auftragsverarbeitern .....	102
f) Bestellung eines Datenschutzbeauftragten .....	103
g) Verhaltensregeln und Zertifizierungen .....	104
2. BDSG (neu) .....	105
3. ePrivacy-Verordnung (Entwurf) .....	105
<b>IV. Response</b> .....	106
1. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde .....	106
2. Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person .....	110

<b>V. Rechtmäßigkeit der Verarbeitung personenbezogener Daten bei der Durchführung von Cyber-Sicherheitsmaßnahmen</b> . . . . .	112
1. Zulässigkeit der Verarbeitung personenbezogener Daten nach DSGVO . . . . .	112
a) Notwendigkeit einer Rechtsgrundlage . . . . .	112
b) Einwilligung der betroffenen Personen . . . . .	113
c) Erfüllung rechtlicher Pflichten . . . . .	113
d) Wahrnehmung berechtigter Interessen . . . . .	114
e) Folgen einer unzulässigen Verarbeitung . . . . .	115
2. Mögliche zusätzliche Anforderungen . . . . .	115
a) TKG . . . . .	115
b) BetrVG . . . . .	116
<b>VI. Sanktionen</b> . . . . .	116
1. Verhängung von Geldbußen . . . . .	116
2. Haftung und Recht auf Schadensersatz . . . . .	118
3. Befugnisse der Aufsichtsbehörde . . . . .	119

**Kapitel 5  
IT-Sicherheit**

*Prof. Dr. Norbert Wimmer/Robert Mechler*

<b>I. Rechtliche Grundlagen</b> . . . . .	123
<b>II. Preparedness</b> . . . . .	127
1. Pläne und Strategien zur Verbesserung der IT-Sicherheit in Deutschland . . . . .	127
2. Pflichten zur Sicherung von IT-Anlagen privatwirtschaftlicher Unternehmen . . . . .	128
a) Präventive Maßnahmen gem. BSIG . . . . .	128
b) Präventive Befugnisse des BSI . . . . .	134
c) Spezialgesetzliche Regelungen zur IT-Sicherheit . . . . .	137
3. Die Implementierung von IT-Sicherheit im Unternehmen . . . . .	143
4. Pflichten zur Sicherung von IT-Anlagen im Sektor Staat und Verwaltung . . . . .	144
a) Vorgaben des BSIG . . . . .	144
b) Vorgaben des UP Bund . . . . .	146
c) Kommunikationsnetze des Bundes . . . . .	147
d) Vorgaben des Online-Zugangsgesetzes . . . . .	148

Inhaltsverzeichnis

<b>III. Response</b> .....	149
1. Meldepflichten von Betreibern kritischer Infrastrukturen .....	149
a) Meldeverpflichtung .....	149
b) Meldungsinhalt .....	150
2. Meldepflichten von Anbietern digitaler Dienste .....	151
3. Bewältigung von Störungen und Befugnisse des BSI .....	152
4. Spezialgesetzliche Meldepflichten .....	154
a) Meldepflichten im Energierecht .....	154
b) Meldepflichten im Atomrecht .....	154
c) Meldepflichten im Telekommunikationsrecht .....	155
d) Meldepflichten im Recht der Telemediendienste .....	157
e) Meldepflichten für die Gesellschaft für Telematik .....	157
5. Meldepflichten und Störungsbewältigung im Sektor Staat und Verwaltung .....	157
<b>IV. Sanktionen</b> .....	158
1. Sanktionsvorschriften des BSI .....	158
2. Sanktionsvorschriften aus Spezialgesetzen .....	158
3. Einfluss auf das Zivilrecht .....	159
<b>V. Ausblick: IT-Sicherheitsgesetz 2.0</b> .....	160

**Kapitel 6**  
**Arbeitsrecht**

*Hendrik Röger*

<b>I. Arbeitsrechtliche Grundlagen</b> .....	164
1. Individualarbeitsrecht .....	164
a) Beschäftigung als Verantwortlicher für Cyber-Security .....	164
b) Handlungspflichten aus Cyber-Security-Richtlinien .....	165
c) Arbeitsvertragliche Nebenpflichten .....	167
2. Kollektivarbeitsrecht .....	168
a) Beteiligungsrechte von Betriebsräten .....	168
b) Mitbestimmung in Cyber-Security-Notfällen .....	168
<b>II. Kollisionsrecht</b> .....	171
<b>III. Preparedness</b> .....	172
1. Cyber-Security-Richtlinien .....	172
a) Inhalt und Form .....	173
b) Individualarbeitsrechtliche Pflichten .....	173



## Inhaltsverzeichnis

c) Beteiligungsrechte des Betriebsrats. ....	174
2. Schulung und Lernkontrolle („train & test“). ....	175
a) Schulung und Kontrolle . . . . .	175
b) Individualarbeitsrechtliche Pflichten . . . . .	176
c) Beteiligungsrechte des Betriebsrats. ....	177
3. Umgestaltung der Arbeitsumgebung . . . . .	177
<b>IV. Response</b> . . . . .	179
1. Response-Richtlinien . . . . .	179
a) Inhalte von Response-Richtlinien . . . . .	179
b) Individualarbeitsrechtliche Pflichten . . . . .	179
c) Beteiligungsrechte des Betriebsrats. ....	180
2. Abwehrmaßnahmen . . . . .	180
a) Typische Abwehrmaßnahmen . . . . .	180
b) Individualarbeitsrechtliche Pflichten . . . . .	181
c) Beteiligungsrechte des Betriebsrats. ....	181
<b>V. Sanktionen</b> . . . . .	184
1. Disziplinarische Maßnahmen. ....	184
a) Ermahnung/Abmahnung . . . . .	184
b) Kündigung . . . . .	184
2. Schadensersatz . . . . .	185
a) Pflichtverletzung . . . . .	185
b) Grundsätze der Haftungsbegrenzung für Arbeitnehmer . . . . .	186
c) Mitverschulden des Arbeitgebers aufgrund unzureichender Preparedness . . . . .	188

## Kapitel 7

### Aufsichtsrecht (Banken und Versicherungen)

*Dr. Andreas Wieland*

<b>I. Überblick und rechtliche Grundlagen</b> . . . . .	193
1. Bedeutung für den Finanzsektor. ....	193
2. Cyber-Angriffe im Finanzsektor . . . . .	194
3. Rechtsquellen . . . . .	196
a) Überblick . . . . .	196
b) Nationale Vorgaben. ....	197
c) Europäische und supranationale Vorgaben . . . . .	198

## Inhaltsverzeichnis

<b>II. Preparedness (Anforderungen an das Risikomanagement von Banken)</b> .....	200
1. Kreditwesengesetz (KWG) .....	200
a) Organisatorische Pflichten (§ 25a KWG) .....	201
b) Auslagerungen (§ 25b KWG) .....	201
2. Mindestanforderungen an das Risikomanagement (MaRisk) und Bankaufsichtliche Anforderungen an die IT (BAIT) .....	202
a) Technisch-organisatorische Ausstattung (AT 7.2 MaRisk und BAIT) .....	203
b) Notfallkonzept (AT 7.3 MaRisk, Ziff. 7 BAIT) .....	203
c) Auslagerungen (AT 9 MaRisk, Ziff. 8 BAIT) .....	204
3. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) .....	205
a) Anwendungsbereich .....	206
b) Angemessene organisatorische und technische Vorkehrungen (§ 8a Abs. 1, Abs. 2 BSIG) .....	206
c) Nachweispflicht (§ 8a Abs. 3 BSIG) .....	208
d) Besondere Anforderungen an Anbieter digitaler Dienste (§ 8c BSIG) .....	208
4. Sonstige Publikationen von Aufsichtsbehörden .....	208
a) BaFin-Journal .....	208
b) EBA-Leitlinien .....	209
c) ESMA-Leitlinien .....	210
d) EZB .....	211
<b>III. Response (Meldepflichten der Banken)</b> .....	211
1. BSIG/BSI-KritisV .....	211
a) Anlass der Meldung .....	212
b) Inhalt der Meldung .....	213
c) Unternehmerische Kontaktstelle .....	213
2. Rahmenwerk der EZB .....	214
a) Rechtsnatur .....	214
b) Cyber-Security-Vorfall .....	215
c) Wesentlichkeit .....	215
d) Meldevorlage .....	216
3. KWG, MaRisk und BAIT .....	216
<b>IV. Besondere Anforderungen und Meldepflichten für Zahlungsinstitute und Versicherungen</b> .....	216
1. Zahlungsinstitute .....	217
a) Zahlungsdiensteaufsichtsgesetz (ZAG) .....	217

b) Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI) .....	218
c) BaFin-Rundschreiben zur Meldung schwerwiegender Zahlungssicherheitsvorfälle .....	220
d) BSIG/BSI-KritisV .....	220
e) EBA-Leitlinien .....	220
2. Versicherungsunternehmen .....	221
a) Versicherungsaufsichtsgesetz (VAG) .....	222
b) Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) und Versicherungs- aufsichtlichen Anforderungen an die IT (VAIT) .....	223
c) BSIG/BSI-KritisV .....	223
d) EIOPA-Publikation .....	224
<b>V. Eingriffsmaßnahmen und Sanktionen</b> .....	224
1. Öffentlich-rechtliche Sanktionen .....	224
a) Verstöße gegen das KWG .....	225
b) Verstöße gegen das BSIG .....	225
c) Verstöße gegen das ZAG .....	226
d) Verstöße gegen das VAG .....	226
2. Strafrechtliche Sanktionen .....	226
3. Zivilrechtliche Sanktionen .....	227

## **Kapitel 8 Kartellrecht**

*Dr. Justus Herrlinger*

<b>I. Rechtsgrundlagen</b> .....	229
1. Europäisches Kartellverbot .....	230
2. Deutsches Kartellverbot .....	232
3. „Softlaw“ .....	232
<b>II. Kollisionsrecht</b> .....	233
<b>III. Preparedness</b> .....	234
1. Problembewusstsein: Anwendbarkeit und Risiken des Kartellrechts .....	234
2. Erkennen von Wettbewerbsverhältnissen .....	236
3. Absprachen zwischen Wettbewerbern .....	237
4. Unzulässiger Informationsaustausch .....	238

Inhaltsverzeichnis

<b>IV. Response</b> .....	239
1. Compliance-Schulungen und Aufklärung .....	240
2. „Whistle Blower“ und „Internal Investigation“ .....	240
3. Kronzeugenanträge und sonstige Kooperation mit Kartellbehörden .....	241
<b>V. Sanktionen</b> .....	242
1. Bußgelder .....	242
2. Untersagungsverfügungen .....	243
3. Schadensersatzklagen .....	244

**Kapitel 9**  
**Vergaberecht**

*Dr. Lars Ole Petersen*

<b>I. Rechtliche Grundlagen</b> .....	245
<b>II. Preparedness</b> .....	246
1. Gewährleistung der Vertraulichkeit durch die öffentliche Hand .....	247
a) Betriebs- und Geschäftsgeheimnisse .....	247
b) Besonders geschützte Unterlagen .....	248
c) Schutzniveau und Maßnahmen .....	249
2. Gewährleistung der Vertraulichkeit durch den Bieter .....	251
3. Umgang mit No-Spy-Erlass und dessen Auswirkungen .....	252
<b>III. Response</b> .....	254
1. Cyberbedingter Bruch der Vertraulichkeit beim Bieter .....	254
a) Reaktion des Bieters .....	254
b) Reaktion des öffentlichen Auftraggebers .....	254
2. Cyberbedingter Bruch der Vertraulichkeit beim öffentlichen Auftraggeber .....	255
a) Reaktion des öffentlichen Auftraggebers .....	255
b) Reaktion des Bieters .....	257
<b>IV. Rechtsfolgen</b> .....	257
1. Cyberbedingter Bruch der Vertraulichkeit beim Bieter .....	257
a) Ausschluss .....	257
b) Haftung .....	258
2. Cyberbedingter Bruch der Vertraulichkeit beim öffentlichen Auftraggeber .....	258

a) Neustart des Verfahrens .....	258
b) Haftung .....	259
3. Cyberbedingter Bruch der Vertraulichkeit durch einen Bieter ...	259

**Kapitel 10**  
**Prozessführung und Haftung**

*Markus Langen, LL.M. (Sydney)/Dr. Dominik Stier*

<b>I. Einleitung .....</b>	<b>262</b>
<b>II. Rechtsvergleichender Überblick – Litigation-Trends</b>	
<b>in den USA. ....</b>	<b>263</b>
1. Target – Der Wendepunkt .....	264
2. Ashley Madison – „Christmas in September“? .....	265
3. Yahoo – First data breach related securities class action .....	266
4. Equifax – Avalanche of Litigation .....	267
5. Zusammenfassende Würdigung und Schlussfolgerung	
für Deutschland .....	268
a) Consumer Litigation .....	268
b) Financial Institution Litigation .....	269
c) Securities Litigation .....	270
d) Directors & Officers Litigation .....	270
e) Schlussfolgerungen für Deutschland .....	271
<b>III. Zivilrechtliche Haftungsrisiken für das Unternehmen in</b>	
<b>Deutschland .....</b>	<b>271</b>
1. Vertragliche Ansprüche .....	271
a) Schadensersatz wegen Verletzung vertraglicher	
Primärleistungspflichten .....	271
b) Schadensersatz wegen Verletzung vertraglicher	
Nebenpflichten .....	272
c) Haftung von Banken bei Überweisungen im Online-Banking	274
d) Schadensersatzansprüche von Banken gegen	
Einzelhandelsunternehmen .....	275
2. Haftung aus Delikt .....	276
a) Schadensersatz wegen Verletzung der DSGVO .....	276
b) Schadensersatz wegen Verletzung des TKG .....	278
c) Haftung für Rechtsverletzungen Dritter .....	278
d) Kapitalmarktrechtliche Haftung .....	278
e) Allgemeine Deliktshaftung .....	279

Inhaltsverzeichnis

<b>IV. Haftung der Geschäftsleiter</b> .....	280
<b>V. International zuständige Gerichte</b> .....	281
<b>VI. International anwendbares Recht</b> .....	283
1. Vertragliche Haftungsansprüche .....	283
2. Deliktische Haftungsansprüche .....	284
<b>VII. Kollektive Rechtsverfolgung</b> .....	284
<b>VIII. Fazit/Ausblick</b> .....	285

**Kapitel 11**  
**Strafrecht**

*Karl-Jörg Xylander/Tobias Gans*

<b>I. Vorbemerkung</b> .....	288
1. Strafbarkeit von Cyber-Angriffen .....	289
a) Spionageangriffe .....	290
b) Sabotageangriffe .....	293
c) Betrügerische Angriffe auf das Vermögen und rechtserhebliche Datenvorgänge .....	295
d) Strafbare Vorbereitungshandlungen .....	296
e) Voraussetzungen der Strafverfolgung .....	297
2. Straf- und Bußgeldrisiken für Unternehmensverantwortliche im Zusammenhang mit Cyber-Angriffen .....	298
a) Unzureichende Absicherung von Daten .....	298
b) Verletzung gesetzlicher Melde- und Informationspflichten ..	302
c) Straf- und Ordnungswidrigkeitsrisiken bei besonderen Gefährdungslagen .....	304
<b>II. Zusammenarbeit mit Ermittlungs- und Fachbehörden sowie sonstigen Dritten</b> .....	305
1. Gründe für die Zusammenarbeit mit den Ermittlungsbehörden ..	305
a) Expertise und Eingriffsbefugnisse der Ermittlungsbehörden ..	305
b) Vorbereitung eines Zivilprozesses und Sicherung von Beweisen .....	306
2. Zu beachtende Risiken .....	306
a) Drohender Reputationsschaden .....	306
b) Sicherstellung oder Beschlagnahme von Beweismitteln von Hard- und Software .....	306

c) Umschwenken von ökonomisch motivierten Taten in Sabotagehandlungen . . . . .	307
3. Einschaltung von Fachbehörden und sonstigen Dritten . . . . .	307
<b>III. Straf- und Verfolgbarkeit von Auslandstaaten . . . . .</b>	<b>308</b>
1. Anwendbarkeit des deutschen Strafrechts . . . . .	308
2. Grenzüberschreitende Ermittlungen . . . . .	310
<b>IV. Kriminalitätsstatistiken und Aufklärungsrate . . . . .</b>	<b>312</b>

**Kapitel 12**  
**Versicherungsrecht**

*Christian Wirth*

<b>I. Grundlagen . . . . .</b>	<b>316</b>
1. Begriff . . . . .	318
2. Häufigste Gestaltungsform . . . . .	318
3. Überblick über die Cyber-Risiken und deren Ursachen . . . . .	319
4. Marktentwicklung und Bedingungswerke . . . . .	320
a) Gesetzgeberische Aktivitäten . . . . .	320
b) Bedingungswerke . . . . .	321
<b>II. Preparedness . . . . .</b>	<b>322</b>
1. Sachlicher Gegenstand einer Cyber-Versicherung . . . . .	323
a) Drittschäden . . . . .	323
b) Eigenschäden . . . . .	324
2. Versicherungsfall . . . . .	325
a) Schadensereignisprinzip . . . . .	327
b) Claims-made-Prinzip . . . . .	327
c) Kausalereignisprinzip . . . . .	328
3. Umfang des Versicherungsschutzes . . . . .	328
a) Haftpflicht . . . . .	328
b) Vermögenseigenschäden . . . . .	329
c) Zusätzliche Deckungsmöglichkeiten . . . . .	329
4. Risikoausschlüsse . . . . .	335
5. Obliegenheiten vor Eintritt des Versicherungsfalls . . . . .	336
a) Gesetzliche Obliegenheiten vor Eintritt des Versicherungsfalls . . . . .	337
b) Vertragliche Obliegenheiten vor Eintritt des Versicherungsfalls . . . . .	340
6. Deckungssummen . . . . .	342

Inhaltsverzeichnis

7. Überschneidungen mit anderen Versicherungspolicen .....	342
a) Betriebshaftpflichtversicherung .....	343
b) (Feuer-)Betriebsunterbrechungsversicherung .....	343
c) Vertrauensschadenversicherung .....	344
d) D&O-Versicherung.....	344
e) W&I-Versicherung .....	345
f) Strafrechtsschutzversicherung.....	345
8. Pflicht zum Abschluss einer Cyber-Risk-Versicherung durch die Unternehmensleitung? .....	346
<b>III. Response</b> .....	346
1. Gesetzliche Obliegenheiten nach Eintritt des Versicherungsfalls .	347
a) § 82 VVG.....	347
b) § 31 VVG.....	347
2. Vertragliche Obliegenheiten nach Eintritt des Versicherungsfalls.....	348
3. Besonderheiten in tatsächlicher Hinsicht beim Nachweis des Versicherungsfalls im Rahmen der Cyber-Deckung – Optimierungsmöglichkeiten.....	348

**Kapitel 13**  
**Länderbericht USA**

*Steven Chabinsky/F. Paul Pittman/David Markoff/Mark Williams*

<b>I. Introduction</b> .....	353
<b>II. Corporate Law</b> .....	354
<b>III. Corporate Transactions (M&amp;A)</b> .....	355
<b>IV. Data Protection and Data Breach Requirements</b> .....	357
<b>V. IT Security Law and Industry Standards</b> .....	359
<b>VI. Criminal Law</b> .....	360
<b>VII. IT Outsourcing and Commercial Contracts</b> .....	362
<b>VIII. Employment Law</b> .....	364
<b>IX. Regulatory</b> .....	365
<b>X. Public Law (incl. Procurement)</b> .....	367
<b>XI. Information Sharing and Antitrust Law</b> .....	368



**XII. Insurance** ..... 369  
**XIII. Impact/Influence of Extraterritorial Law** ..... 369

**Kapitel 14  
Länderbericht UK**

*Dr. Philip Trillmich/John Timmons*

**I. Overview** ..... 372  
1. Applicable Laws ..... 373  
2. Territorial Application ..... 374  
3. General Legal Liabilities ..... 374  
a) Negligence ..... 374  
b) Misuse of Private Information ..... 375  
4. General Cybersecurity Practices ..... 375  
5. Cybersecurity-related Bodies and Guidance ..... 376  
a) The National Cyber Security Centre ..... 376  
b) The Information Commissioner’s Office ..... 377  
c) Others ..... 377  
**II. Corporate Law** ..... 378  
1. Preparedness ..... 378  
a) General Obligations on all Organisations ..... 378  
b) Directors’ Duties ..... 379  
2. Response ..... 381  
3. Legal Liabilities ..... 381  
**III. M&A/Due Diligence** ..... 382  
1. General ..... 382  
2. Preparedness ..... 382  
a) General ..... 382  
b) Due Diligence Process ..... 382  
3. Responses ..... 383  
**IV. Data Protection** ..... 384  
1. General ..... 384  
2. Definition of Personal Data and Processing ..... 384  
3. Regulator Enforcement and Criminal Offences ..... 385  
4. Preparedness ..... 386  
a) Security of Personal Data ..... 386  
b) Policy Requirements ..... 387

Inhaltsverzeichnis

c) Use of Processors .....	387
5. Responses .....	388
a) Breach Notification .....	388
b) Remedial Actions .....	388
<b>V. Cybersecurity Law .....</b>	<b>388</b>
1. General .....	388
2. Preparedness .....	389
a) In-Scope Organisations .....	389
b) Key Obligations .....	389
c) Legal Liabilities .....	390
3. Responses .....	391
<b>VI. Criminal Law .....</b>	<b>391</b>
1. General .....	391
2. Offences .....	392
a) The CMA 1990 Offences .....	392
b) Legal Liabilities .....	393
3. Notification .....	393
<b>VII. Communications .....</b>	<b>394</b>
1. General .....	394
2. Preparedness .....	394
a) Key Obligations .....	394
b) Legal Liabilities .....	395
3. Responses .....	396
<b>VIII. Employment Law .....</b>	<b>396</b>
1. General .....	396
2. Employee Monitoring .....	397
<b>IX. Financial Services .....</b>	<b>398</b>
1. Overview .....	398
2. Preparedness .....	398
a) FCA Requirements .....	398
b) PRA Requirements .....	399
3. Responses .....	399
a) FCA Notification .....	399
b) PRA Notification .....	400
<b>X. Public Authorities .....</b>	<b>400</b>
1. General .....	400
2. Official Secrets Act 1989 .....	400

<b>XI. Competition Law</b> .....	400
<b>XII. Litigation</b> .....	400

**Kapitel 15**  
**Länderbericht China**

*Melody Chan/Douglas Tan/Denise Cheung/Aurora Leung*

<b>I. Introduction</b> .....	402
1. Network Operators and Critical Information Infrastructures. ....	403
a) Network Operators .....	404
b) Critical Information Infrastructures. ....	404
2. Extraterritorial Reach .....	405
3. Legal Liabilities. ....	405
4. Looking Forward .....	406
<b>II. Corporate Law</b> .....	407
<b>III. M&amp;A</b> .....	407
<b>IV. Data Protection</b> .....	408
1. General .....	408
2. Preparedness .....	408
a) Personal Information Management System .....	408
b) Collection of Personal Information .....	409
c) Storage and Security .....	409
d) Use of Personal Information .....	410
e) Data Localisation for CIIs .....	410
f) Transfer of Personal Information .....	410
g) Disclosure of Personal Information .....	411
h) Deletion of Personal Information .....	411
3. Response .....	411
a) Breach Notification .....	411
b) Take Remedial Actions .....	412
<b>V. IT Security Law</b> .....	413
1. General .....	413
2. Preparedness .....	413
a) General Obligations of All Network Operators .....	413
b) Additional Obligations of CII Operators .....	414
c) Purchasing Network Products and Services .....	414
d) Inspections of Internet Service Providers .....	415

Inhaltsverzeichnis

e) Obligations of Providers of Internet Information Services with the Attribute of Public Opinion or the Ability of Social Mobilization .....	416
3. Response .....	417
<b>VI. Criminal Law .....</b>	<b>417</b>
1. General .....	417
a) Crime of infringing personal information of citizens. ....	418
b) Crime of refusing to perform obligations for security management of information networks. ....	418
c) Crime of illegally using information networks. ....	418
2. Preparedness .....	419
3. Response .....	419
<b>VII. IT, Outsourcing and Commercial Contracts .....</b>	<b>419</b>
1. General .....	419
2. Preparedness .....	420
a) Obtain Data Subject's Consent. ....	420
b) Conduct Security Assessment .....	420
c) Be Mindful of the Purposes behind the Transfer. ....	421
3. Response .....	421
a) Revise Cross-Border Data Transfer Plan. ....	421
b) Take Measures to Lower Security Risks .....	421
<b>VIII. Employment Law .....</b>	<b>422</b>
1. General .....	422
2. Preparedness .....	422
a) Storage and Security .....	422
b) Data Localisation .....	423
3. Response .....	423
a) Data Deletion & Correction .....	423
b) Breach Notification and Remedial Actions .....	423
<b>IX. Regulatory .....</b>	<b>423</b>
1. Financial Institutions .....	424
a) General .....	424
b) Preparedness .....	424
c) Response .....	426
2. Insurance Companies .....	426
a) General .....	426
b) Preparedness .....	427
c) Response .....	428

3. Healthcare and Medical Institutions .....	429
a) General.....	429
b) Preparedness .....	429
c) Response .....	430
4. Power Industry .....	430
a) General.....	430
b) Preparedness .....	431
<b>X. Public Law (incl. Procurement).....</b>	<b>431</b>
<b>XI. Antitrust Law .....</b>	<b>432</b>
<b>XII. Litigation.....</b>	<b>432</b>
<b>XIII. Insurance.....</b>	<b>432</b>

**Kapitel 16  
Checklisten**

*Dr. Alexander Kiefner/Dr. Tobias A. Heinrich, LL.M. (London)*

<b>I. Vorbemerkung .....</b>	<b>436</b>
<b>II. Preparedness .....</b>	<b>436</b>
1. Allgemein/interne Prozesse/Unternehmensorganisation .....	436
a) Risikoanalyse .....	436
b) Folgerungen aus der Risikoanalyse .....	438
c) Unternehmensorganisation und -leitung .....	439
2. Datenschutzrecht .....	441
3. IT-Sicherheitsrecht .....	442
a) Betreiber von Kritischen Infrastrukturen bzw. Anbieter digitaler Dienste .....	442
b) Anlage mit Energiebezug .....	443
c) Anlage mit Atombezug .....	443
d) Telekommunikations- und Telemedienanbieter .....	444
4. Arbeitsrecht .....	444
5. Aufsichtsrecht .....	445
a) Anforderungen an das Risikomanagement von Banken .....	445
b) Anforderungen an das Risikomanagement bei Kritischen Infrastrukturen .....	446
c) Anforderungen an das Risikomanagement von Zahlungsinstituten .....	446

## Inhaltsverzeichnis

d) Anforderungen an das Risikomanagement von Versicherungen .....	446
6. Kartellrecht .....	447
7. Vergaberecht .....	448
a) Gewährleistung der Vertraulichkeit durch die öffentliche Hand .....	448
b) Gewährleistung der Vertraulichkeit durch den Bieter .....	449
8. Versicherungsrecht .....	450
a) Allgemein .....	450
b) Obliegenheiten des Versicherungsnehmers vor Eintritt eines Versicherungsfalls .....	451
<b>III. Response</b> .....	452
1. Cyber Incident Response Plan (CIRP) .....	452
2. Response-Team .....	455
3. Gesellschaftsrecht (Unternehmensleitung und Unternehmensorganisation) .....	455
a) Entscheidung über die konkrete Reaktion/Business Judgment Rule .....	455
b) Insiderrecht/Ad-hoc-Publizität (börsennotierte Unternehmen) .....	456
c) Nachgelagerte Maßnahmen .....	456
4. Datenschutzrecht .....	457
5. Arbeitsrecht .....	457
6. Kartellrecht .....	457
7. Vergaberecht .....	458
a) Bietersicht .....	458
b) Öffentlicher Auftraggeber .....	458
8. Strafrecht .....	459
9. Versicherungsrecht .....	460
Stichwortverzeichnis .....	461