

# INHALT

Vorwort von Peter Gleason	11
Vorwort von Sebastian Lange	15
Vorbemerkung	19
Über die Autoren	23

## 1 Cybersicherheit ist (nicht) ein IT-Problem

Fünf wichtige Erkenntnisse, die Sie aus diesem Kapitel mitnehmen können	27
Einleitung	27
Warum wir bei der Sicherung des Cyberspace keine Fortschritte machen	29
Die digitale Transformation macht Cybersicherheit zu einem Businesssthema	31
Die neue Grenze: Künstliche Intelligenz (KI) und Angriffe, die lernen	34
Warum es schwierig ist, Unternehmenswachstum, Rentabilität und Cybersicherheit in Einklang zu bringen	39
Die Covid-19-Pandemie: Cybergestützte Unternehmen und erhöhtes Risiko	40
Das Cybersicherheitsproblem ist ernst und wird schnell gravierender	42
Technische Schwachstellen sind ein Problem – aber nicht das einzige Problem	44
Warum Cyber-Infrastrukturen angegriffen werden – folgen Sie dem Geld	47
Die Wirtschaftlichkeit der Cybersicherheit steht auf dem Kopf	49
Das wirtschaftliche Gleichgewicht im Cyberspace begünstigt die Angreifer	52
Gute Cyberhygiene ist nicht genug	53
Sicherheit vs. Compliance	57
Das Sanktionsmodell zur Erzwingung angemessener Sicherheit	59
Was kann ein Unternehmen für die Cybersicherheit tun?	61
Schlussfolgerung	64

## 2 Wirksame Cybersicherheitsgrundsätze für das Board

Fünf wichtige Erkenntnisse, die Sie aus diesem Kapitel mitnehmen können	67
Einleitung	67

Welche Rolle spielt das Board bei der Cybersicherheit?	68
Wie sich das Denken des Boards über Cybersicherheit entwickelt hat	68
Entwicklung und Validierung von Grundsätzen für die Cybersicherheit auf Ebene des Boards	71
Prozess zur Entwicklung der internationalen Grundsätze für Boards und Cybersicherheit	75
Fünf übereinstimmende Grundsätze für effektive Cybersicherheit auf Ebene des Boards	77
Erläuterung der Grundsätze der Cybersicherheit im Board	79
Schlussfolgerung	89

### **3 Strukturierung für das digitale Zeitalter**

Fünf wichtige Erkenntnisse, die Sie aus diesem Kapitel mitnehmen können	93
Einleitung	93
Die Abkehr von digitalen Silos	94
Schaffung eines Managementrahmens für die Cybersicherheit	95
Wir sind noch nicht integriert	96
Abgeschottete Cybersicherheitssysteme sind kontraproduktiv	98
Wie zentralisiert sollte der Aufgabenbereich Cybersicherheit sein?	99
Wem ist der Leiter der Cybersicherheitsabteilung unterstellt?	101
Wer gehört zum Cybersicherheitsteam?	103
Die richtige Struktur für das Cybersicherheitsteam finden	109
Anpassung der Unternehmensarchitektur	110
In der Finanzdienstleistungsbranche initiierte Kooperationsmodelle	111
Schlussfolgerung	114

### **4 Ein moderner Ansatz zur Bewertung von Cyberrisiken**

Fünf wichtige Erkenntnisse, die Sie aus diesem Kapitel mitnehmen können	119
Einleitung	119

# CYBERSICHERHEIT FÜR UNTERNEHMEN

Was ist ein Cyberrisiko? 121

Vergleich traditioneller Cyberrisiko-Methoden 123

Eine bessere Herangehensweise 126

Die moderne Risikobewertung 127

Vereinfachen Sie die Betrachtung von Cyberrisiken 128

Übersetzung traditioneller Cybersicherheitskennzahlen in finanzielle Details 131

Bereitstellung eines Instruments für eine standardisierte und wiederholbare Cyberrisiko-Bewertung 134

Prognostizierte finanzielle Belastung durch Cyberrisiken 138

Bereitstellung einer Reihe von priorisierten Abhilfe- und Transferanleitungen 140

Cyberrisiko mit unternehmensweisem Risikomanagement-Berichtswesen abstimmen 145

Schlussfolgerung 145

## **5 Die Rolle der Personalabteilung bei der Skalierung der Cybersicherheit und dem Aufbau von Vertrauen**

Fünf wichtige Erkenntnisse, die Sie aus diesem Kapitel mitnehmen können 151

Einleitung 152

Bedrohung durch Insider: Die Achillesferse 153

Telearbeit: Die neueste Komplikation 157

Entwicklung einer sicherheitsorientierten Unternehmenskultur 159

Entwicklung von Prozess- und Betriebskontrollen 161

Der Wert der Personalarbeit im Bereich der Cybersicherheit 162

Anwerbung, Einstellung und Bindung 166

Ausbildung: Eine ständige Verpflichtung für die Sicherheit 170

Austrittsprozess 172

Schlussfolgerung 173

## **6 Cybersicherheit und die Rechtsabteilung**

Fünf wichtige Erkenntnisse, die Sie aus diesem Kapitel mitnehmen können 177

Einleitung 178

Warum die Cybersicherheit ein proaktives Vorgehen des Justizars erfordert 179

Hauptverantwortlichkeiten – die Grundlagen 180

Überwachung und Beratung bei Änderungen der gesetzlichen, regulatorischen und branchenspezifischen Anforderungen 181  
Regulatorische Anforderungen 182  
Die Rolle des Justiziaris im Cybersicherheits-Risikomanagement 194  
Schlussfolgerung 200

## **7 Überlegungen zu Cybersicherheitsprüfung und Compliance**

Fünf wichtige Erkenntnisse, die Sie aus diesem Kapitel mitnehmen können 203  
Einleitung 204  
Die aktuelle Landschaft der Compliance- und Prüfungsanforderungen 205  
Einhaltung der Cybersicherheitsvorschriften im Rahmen des Risikomanagements von Unternehmen 212  
Die Rolle des Audits 214  
Das Modell der drei Verteidigungslinien 217  
Die Rolle der externen Auditoren 219  
Die Rolle der Technologie bei zukünftigen Compliance- und Auditmaßnahmen 221  
Schlussfolgerung 224

## **8 Cyberrisiko-Management für die Lieferkette und für Drittparteien**

Fünf wichtige Erkenntnisse, die Sie aus diesem Kapitel mitnehmen können 229  
Einleitung 229  
Herangehensweise an das Cyberrisiko-Management für die Lieferkette 231  
Berücksichtigung von Cybersicherheitsmanagement und IT-Governance bei der Berechnung der Gesamtbetriebskosten 232  
Verhandlungsstrategien unter Einbeziehung von Cybersicherheits-Versicherungsbestimmungen 235  
Umsetzung inklusiver Service-Level-Agreements 237  
Einbeziehung der Cybersicherheit in das aktuelle Risikomanagement der Lieferkette 239  
Schulung der Mitarbeiter der Lieferkette zur Erkennung von Cybersicherheitsrisiken und zur Durchführung von Maßnahmen zur Risikominderung 240

## **CYBERSICHERHEIT FÜR UNTERNEHMEN**

- Due Diligence von Cyberlieferketten-Drittanbietern 242
- Einbeziehung von Cyberanforderungen in das Risikomanagementprogramm für Dritte 249
- Sicherstellung, dass Vereinbarungen mit Cyberdrittanbietern angemessene Kontrollen für rechtliche Risiken und Compliance bieten 251
- Schlussfolgerung 252

### **9 Technischer Betrieb**

- Fünf wichtige Erkenntnisse, die Sie aus diesem Kapitel mitnehmen können 255
- Einleitung 256
- Technische Transaktionen – die Notwendigkeit einer konsequenten Koordinierung von „Defense in Depth“ 257
- Prävention – technische Maßnahmen 262
- Erkennung – technische Maßnahmen 264
- Reaktion – technische Maßnahmen 279
- Schlussfolgerung 283

### **10 Krisenmanagement**

- Fünf wichtige Erkenntnisse, die Sie aus diesem Kapitel mitnehmen können 289
- Einleitung 289
- Was ist ein Plan zur Reaktion auf Zwischenfälle (IRP)? 293
- Warum brauchen Sie einen Plan? 294
- Unternehmerische Fähigkeiten und Aufgabenbereiche, die zur Unterstützung der Reaktion auf Vorfälle erforderlich sind 295
- Fragen, die die Geschäftsleitung bei der Ausarbeitung eines IRP berücksichtigen sollte 297
- Zu benachrichtigende Dritte 313
- Schlussfolgerung 315

## **11 Überlegungen zur Cybersicherheit während der M&A-Phasen**

Fünf wichtige Erkenntnisse, die Sie aus diesem Kapitel mitnehmen können 319

Einleitung 320

Wann ist der beste Zeitpunkt für die Durchführung der Risikobewertung in puncto M&A? Je früher, desto besser 322

Strategie- und Zielfindungsphase 324

Due-Diligence- und Abwicklungsphase 328

Integrationsphase 332

Schlussfolgerung 335

## **12 Aufbau von Beziehungen mit dem Cybersicherheitsteam**

Fünf wichtige Erkenntnisse, die Sie aus diesem Kapitel mitnehmen können 339

Einleitung 340

Eine gesunde Unternehmenskultur 342

Einfühlungsvermögen: Die Gefühle anderer zu verstehen ist Teil der Cybersicherheit 343

Die Rolle des CISO 345

Beziehungen zum Cybersicherheitsteam 348

Beziehungen innerhalb des Unternehmens 350

Beziehungen außerhalb des Unternehmens 354

Leistung bewerten 355

Schlussfolgerung 359

Endnoten 363