

LARRY CLINTON  
(HRSG.)



# CYBER SICHER HEIT FÜR UNTER NEHMEN

Profi-Strategien zur  
Abwehr von Gefahren  
aus dem Netz

**Exklusives  
Vorwort**

für die dt. Ausgabe  
von Sebastian Lange,  
CSO von SAP

PLASSEN  
VERLAG



**CYBERSICHERHEIT FÜR UNTERNEHMEN  
LARRY CLINTON**

Die Originalausgabe erschien unter dem Titel  
„Cybersecurity for Business“ bei Kogan Page Limited.  
ISBN 978-1-398-60614-2

Copyright der Originalausgabe 2022:  
Copyright © Larry Clinton, 2022  
Copyright © Internet Security Alliance, 2022  
All rights reserved.  
This translation of Cybersecurity for Business is published by arrangement  
with Kogan page.

Copyright der deutschen Ausgabe 2024:  
© Börsenmedien AG, Kulmbach

Übersetzung: Börsenmedien AG  
Coverfoto: Shutterstock  
Gestaltung und Satz: Sabrina Slopek  
Vorleser: Sebastian Politz  
Korrektorat: Rotkel. Die Textwerkstatt  
Druck: GGP Media GmbH, Pößneck

ISBN 978-3-86470-949-4

Alle Rechte der Verbreitung, auch die des auszugsweisen Nachdrucks,  
der fotomechanischen Wiedergabe und der Verwertung durch Datenbanken  
oder ähnliche Einrichtungen vorbehalten.

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

 **BÖRSEN MEDIEN**  
AKTIENGESELLSCHAFT

Postfach 1449 • 95305 Kulmbach  
Tel: +49 9221 9051-0 • Fax: +49 9221 9051-4444  
E-Mail: [info@plassen-buchverlage.de](mailto:info@plassen-buchverlage.de)  
[www.plassen.de](http://www.plassen.de)  
[www.facebook.com/plassenbuchverlage](https://www.facebook.com/plassenbuchverlage)  
[www.instagram.com/plassen\\_buchverlage](https://www.instagram.com/plassen_buchverlage)

LARRY CLINTON (HRSG.)

**CYBER  
SICHER  
HEIT  
FÜR  
UNTER  
NEHMEN**

PROFI-STRATEGIEN  
ZUR ABWEHR VON  
GEFAHREN AUS  
DEM NETZ

PLASSEN  
VERLAG

# 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 Businessstema 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 unternehmensweitem 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



# WEGWEISER DURCH DIE GRAUZONE

VON PETER GLEASON, PRÄSIDENT UND  
GESCHÄFTSFÜHRER, NATIONALER VERBAND  
DER UNTERNEHMENSLEITER

Wenn es um Unklarheiten und Risiken geht, sind nur wenige Führungskräfte besser mit der Herausforderung vertraut, fundierte Ratschläge zu erteilen, als die Leiter von Unternehmen auf der ganzen Welt. Die Mitglieder von Organisationen wie der National Association of Corporate Directors (NACD) und der Internet Security Alliance (ISA) suchen nach einer Orientierungshilfe, mit der sie die Bedrohung durch Cyberangriffe überblicken und ihre Organisationen dementsprechend leiten können. Dabei müssen sie mit einer zunehmenden Bandbreite von Grautönen rechnen – und zwar im Hinblick darauf, wie sie reagieren und wen sie alarmieren sollen und was getan werden kann, um sich vor diesem existenziellen Risiko zu schützen.

In einem Blogbeitrag vom Dezember 2020 bezeichnete Elizabeth Braw, Gastwissenschaftlerin am American Enterprise Institute, den Datendiebstahl durch nordkoreanische, staatlich gesponserte Hacker bei einem der am Projekt „Warp Speed“ beteiligten Unternehmen als „Grauzonen“-Kriegsführung. Eine kurze Suche nach dem Begriff zeigt bereits, dass unter Außenpolitikern und Sicherheitsforschern

## CYBERSICHERHEIT FÜR UNTERNEHMEN

Uneinigkeit darüber herrscht, wie dieser Begriff zu definieren ist. Eines ist aber sicher: Cyberangriffe sind eines von vielen und möglicherweise das beste Werkzeug in der Grauzone, um Unternehmen, die in der traditionell grenzenlosen Welt des Internets tätig sind, Schaden zuzufügen. In einer Welt, in der beispielsweise lebensrettende Impfstoffe und kritische Lieferketten gemeinsam und grenzüberschreitend in der Cloud entwickelt werden, haben bössartige Akteure jeglicher Herkunft die Macht, Menschen und Unternehmen erheblichen Schaden zuzufügen.

Trotz der Bemühungen, sensible Daten zu schützen und auf die Vorschriften verschiedener Nationalstaaten zu reagieren, schwindet international das Vertrauen in Institutionen wie nationale Regierungen und Unternehmen, die mit der Daten- und Netzwerksicherheit betraut sind. Laut einer im Juni 2019 von Pew Research durchgeführten Umfrage unter in den Vereinigten Staaten lebenden Menschen gaben 66 Prozent an, dass die Risiken die Vorteile der gemeinsamen Nutzung von Daten mit der Regierung überwiegen. Dieselbe Gruppe berichtete von einem noch größeren Misstrauen gegenüber Unternehmen. 81 Prozent der Befragten gaben an, dass die Risiken, die damit verbunden sind, dass Unternehmen ihre Daten sammeln dürfen, die möglichen Vorteile überwiegen.

Wirtschaft, Regierung und Gesellschaft stehen zweifellos an einem Scheideweg. Laut dem Global Risk Report des Weltwirtschaftsforums für das Jahr 2020 gibt es einerseits die wirtschaftliche und menschliche Verheißung der vierten industriellen Revolution und all dem, was die damit verbundenen Technologien mit sich bringen können. Andererseits herrschen

in zunehmendem Maße geopolitische Spannungen durch Grauzonen-Taktiken, ein möglicherweise fragmentiertes Internet, verursacht durch Maßnahmen umkämpfter Nationalstaaten, und die daraus resultierende Erstickung von einst vielversprechenden Innovationen. Der Bericht des Forums für das Jahr 2021 stellt fest, dass die geopolitische Frag-

mentierung tatsächlich zu einer Zunahme von Cyberangriffen geführt hat. Wenn unsere Institutionen weiterhin nicht konform mit den anerkannten Governance-Grundsätzen arbeiten, könnten Cyberangriffe in Umfang und Schwere weiter zunehmen.

Die Partnerschaft zwischen der NACD und der ISA zur Entwicklung einer Reihe globaler Cybersicherheitsgrundsätze gibt den Institutionen, die dieses sich ständig verändernde Risiko überwachen, den richtigen Weg vor. In diesem Buch werden diese Grundsätze, die in Kapitel 2 eingehender erörtert werden, auf die Managementebene ausgeweitet. Es bietet eine Anleitung zu spezifischen Prozessen, die aktuelle und angehende Führungskräfte in ihren jeweiligen Bereichen umsetzen sollten, um die Erwartungen ihres Boards an ein solides Management der komplizierten und ständig zunehmenden Cyber-risiko-Herausforderungen in Unternehmen zu erfüllen.

Befassen Sie sich daher bitte mit den in diesem Band erörterten Grundsätzen und bereiten Sie sich darauf vor, sie anzuwenden und in Ihren Boardetagen und darüber hinaus für sie einzutreten. Die Grundsätze zielen darauf ab, die Cyber-Governance für Unternehmen, Anbieter und andere Beteiligte erschwinglicher, effizienter, transparenter und nachvollziehbarer zu machen und zu standardisieren. Es ist noch genug Zeit, den Weg durch die Grauzone schwarz auf weiß aufzuzeigen.

Legen wir los.





# VORWORT

VON SEBASTIAN LANGE,  
SAP CHIEF SECURITY OFFICER

In der Wirtschaft des 21. Jahrhunderts sind Daten von hoher Bedeutung, ähnlich der Rolle von Öl im 20. Jahrhundert. Daten im Zusammenspiel mit Sicherheitsmaßnahmen bilden die Grundlage moderner Unternehmensprozesse. Ob für die Erstellung von Webseiten oder die Rationalisierung von Aufgaben mittels Technologie – Daten werden von Unternehmen genutzt, um Wettbewerber zu überholen und die Produktivität zu steigern. Buchstäblich jeder Unternehmensprozess, jedes System oder jede Anwendung umfasst die Generierung oder Verarbeitung wichtiger Informationen. Die Wahrung des Schutzes von Mitarbeiter-, Kunden- und Betriebsdaten spielt eine erhebliche Rolle, um in der digitalen Wirtschaft erfolgreich zu sein.

Trotz der umfassenden Nutzung von Technologien in Geschäftsprozessen haben viele mit unzureichenden Cybersicherheitsstrategien zu kämpfen. Dieser Missstand entsteht oftmals durch den Irrglauben, dass Cybersicherheit ein rein technisches Anliegen sei. Dieses Vorwort schafft die Voraussetzung für eine Neubewertung dieser zu eng gefassten Perspektive und unterstreicht, wie wichtig es ist, dass das allgemeine Verständnis sich wandelt und der größeren Bedeutung von Cybersicherheit Rechnung trägt. Dieses Buch beschäftigt sich eingehend mit der wachsenden Bedeutung von Cybersicherheit und zeigt auf, wie diese über die Grenzen der IT hinaus sich auf alle Bereiche erfolgreicher Unternehmensführung erstreckt. Cybersicherheit

## CYBERSICHERHEIT FÜR UNTERNEHMEN

betrifft nicht nur technische Experten, sondern jeden, von Berufseinsteigern bis hin zur Unternehmensführung. Dieses Buch verdeutlicht, weshalb sich Cybersicherheit nicht länger nur auf IT beschränkt; sie ist ebenso von Bedeutung für die Geschäftsführung, Rechtsberatung, das Personalwesen und alle weiteren Unternehmensbereiche. Während der Vorstand für Informationstechnologie mit dem Vorstand für Informationssicherheit zusammenarbeitet, um den Schutz des Betriebs zu gewährleisten, strebt der Verwaltungsrat an, eine transformative Unternehmenskultur zu fördern.

Speziell in der heutigen Zeit ist das Fördern einer Sicherheitskultur in Unternehmen eine Priorität für das Personalwesen und dessen Vorstand. Diese Zusammenarbeit dient dazu, das Bewusstsein für und die Einhaltung von Sicherheitsmaßnahmen zu erhöhen. Konkret bedeutet das, dass die Personalabteilung eine zentrale Rolle in der Implementierung von Sicherheitstrainings und der Einhaltung der etablierten Richtlinien spielt. Ihr Mitwirken erstreckt sich von der Vergabe von spezifischen Rollen und Zugangsberechtigungen über Zuverlässigkeitsprüfungen im Einklang mit den Grundsätzen der Cybersicherheit. Bedrohungen wie böswillige Insider, die Exfiltration von Daten und die Ausweitung von Privilegien sind nur einige der Cybersicherheitsrisiken, vor denen Unternehmen ihre Systeme schützen müssen, und das Personalwesen bildet durch die Stärkung der Sicherheitsstellung des Unternehmens die vorderste Abwehrfront.

Unternehmen sind sich bewusst darüber, dass Menschen das schwächste Glied sind, jedoch erfordert das Ändern der Kultur und der Mentalität der Mitarbeitenden nicht nur einen großen Einsatz vonseiten des Personalwesens, sondern ebenso von anderen Funktionsbereichen innerhalb der Organisation. Bei der Förderung einer Sicherheitskultur und dem Etablieren einer Denkweise mit dem Fokus auf Sicherheit handelt es sich wahrlich um funktionsübergreifende Initiativen. Es wird diskutiert, wie Cybersicherheitsrisiken und deren Minderung essenzielle Bestandteile bei der Erstellung einer Strategie für jeden

Funktionsbereich einer Organisation darstellen, ob Rechtsabteilung, das Supply-Chain-Management, Audit und Compliance, Fusions- und Akquisitionsabteilung, Krisenmanagement, Kommunikation oder weitere Bereiche. All diese Funktionen müssen zusammenarbeiten, um eine risikoresistente Cybersicherheitsstrategie zu entwickeln.

Als Nächstes blicken wir auf Compliance und Auditierung. Ebenso wie sich Technologie stetig entwickelt, tun dies auch die damit einhergehenden Risiken. Dies macht eine Weiterentwicklung von Compliance-Konzepten notwendig. Um die Cybersicherheit zu stärken, ist es wichtig, sich auf Unternehmensebene mit Sicherheit zu befassen. Unternehmen müssen daher eine große Menge an Ressourcen für die Einhaltung gesetzlicher Auflagen bei gleichzeitiger Wahrung des Datenschutzes aufwenden. Wirtschaftsprüfung muss über konventionelle Methoden hinausgehen, um umfangreiche Einblicke in unternehmensweite Risiken zu liefern. Trotz der Notwendigkeit von Compliance darf die Einhaltung gesetzlicher Auflagen nicht als einziger Maßstab für Sicherheit dienen.

Im letzten Kapitel wird dargelegt, wie die Zusammenarbeit des Informationssicherheitsteams mit weiteren Funktionsbereichen innerhalb eines Unternehmens, Kunden und weiteren Interessenvertretern gestaltet werden soll, um schlussendlich einen Plan für die Risikomanagement-Richtlinien des Unternehmens zu entwickeln. Für jeden Interessenvertreter steht viel auf dem Spiel, weshalb sie alle in Abstimmung miteinander an einer zuverlässigen Sicherheitskultur arbeiten sollten.

Als Vorstandsmitglieder der Internet Security Alliance schlugen wir eine Reihe an Grundsätzen vor, basierend auf unserem Expertenwissen und unserer langjährigen Erfahrung in der Industrie. Die Effektivität dieser Grundsätze wurde unabhängig durch PwC im Rahmen ihrer Umfrage zur Global Information Security bestätigt. Sie sollen als Basis für die Entwicklung einer Risikomanagement-Richtlinie dienen.

SAP, ein Weltmarktführer im Bereich Enterprise- und Unternehmenssoftware, priorisiert die Sicherheit von Kundendaten und agiert

## CYBERSICHERHEIT FÜR UNTERNEHMEN

im Rahmen einer umfangreichen und unternehmensweiten Sicherheitsstrategie, um zuverlässige und sichere Softwarelösungen anzubieten. Durch die Implementierung der Grundsätze, die in diesem Buch beschrieben werden, möchte SAP die Funktionen von Personen, Prozessen und Technologien für den Aufbau von Vertrauen unterstützen und dabei den Fokus auf Transparenz, Compliance, Sicherheit und Datenschutz legen. Innerhalb der Organisation liegt der Fokus darauf, allen Abteilungen und Mitarbeitenden Trainings zu bieten, statt die Verantwortung für Cybersicherheitsvorkehrungen technischen Teams zu überlassen. Die Sicherheit und der Schutz von Kundendaten genießt bei SAP höchste Priorität.

## VORBEMERKUNG

Dieses Buch ist im Wesentlichen ein Ratgeber für Firmenmanager, der es ihnen ermöglicht, ihre Aktivitäten besser zu verstehen und mit den wachsenden Erwartungen der Boards in Einklang zu bringen, während sie daran arbeiten, die Cyberrisiken ihrer Organisation zu verwalten.

Seit 2014 und bis zum Zeitpunkt der Veröffentlichung und darüber hinaus haben Organisationen, die hinter den Unternehmensvorständen aus der ganzen Welt stehen, Programme durchgeführt, um die Rolle des Boards bei der Beaufsichtigung von Cyberrisiken besser zu verstehen und zu formulieren. Diese Bemühungen haben zu einer Reihe von Handbüchern zum Thema Cyberrisiken geführt, die von diesen Organisationen in Zusammenarbeit mit der ISA erstellt wurden. Der aktuelle Band wurde vom Board der ISA verfasst.

Die Handbücher sind nun auf vier Kontinenten in fünf verschiedenen Sprachen erhältlich. Zwar wurde jedes der Handbücher individuell an die spezifischen Bedürfnisse, die Kultur und die Struktur der verschiedenen Regionen angepasst, aber alle unterstützen die gleichen Grundprinzipien für Boards bei der Wahrnehmung ihrer Aufsichtspflichten in Bezug auf Cyberrisiken.

Wie in Kapitel 2 näher erläutert wird, sind diese Handbücher weltweit von einem breiten Spektrum an Direktoren, Organisationen und Regierungen unterstützt worden. Darüber hinaus wurde die Wirksamkeit der in diesen Handbüchern dargelegten Grundsätze von PwC in

ihrem Global Information Security Survey unabhängig bestätigt. Daher etablieren sich diese Grundsätze zunehmend zum Standard für Führungskräfte in Unternehmen, die sich um die Bewältigung der wachsenden Cyberrisiken bemühen, mit denen Unternehmen konfrontiert sind.

Dieses Buch greift die Grundsätze auf, die Boards bei der Überwachung von Cyberrisiken anwenden, und überträgt sie auf die Führungsebene. Es beginnt mit einer Neukonzeptionierung der Art der Cyberbedrohung. Während man sich bei Cyberbedrohungen traditionell fast ausschließlich auf die technischen Abläufe konzentriert hat, zeigt dieses Buch, dass Cyberrisiken zunehmend als strategisches Geschäftsthema betrachtet werden müssen. Obwohl die technischen Abläufe nach wie vor eine wichtige Rolle bei der Verwaltung von Cyberrisiken spielen, werden die wirtschaftlichen Aspekte der Cybersicherheit immer mehr zu einem entscheidenden Element für das Verständnis der digitalen Transformation in Unternehmen.

Anschließend beschreiben wir, wie Unternehmen dynamische neue Strukturen entwickeln, um multidimensionale Cyberrisiko-Teams zu schaffen, die einen unternehmensweiten und nicht nur einen IT-zentrierten Ansatz für die Cybersicherheit ermöglichen. Auf der Grundlage dieses sich entwickelnden Verständnisses des Boards für Cyberrisiken aus der Geschäftsperspektive und der strukturellen Reformen in den Unternehmen beschreiben wir, wie sich die Bewertung von Cyberrisiken weiterentwickelt – und weiterentwickelt werden muss –, damit Cyberrisiken auf einer empirischen und wirtschaftlichen Grundlage verstanden werden können.

Im Einklang mit dieser sich abzeichnenden unternehmensweiten Anerkennung des Cyberrisiko-Managements erörtern wir anschließend, wie Cyberrisiken nun zu einem Faktor bei einer Vielzahl unternehmerischer Aufgaben und -funktionen werden müssen. Dazu gehört die Rolle des technischen Betriebs, aber auch eine Beschreibung, wie Bereiche wie Personalwesen, Recht, Lieferketten, Audit, Mergers &

Acquisitions, externe Kommunikation und Krisenmanagement jetzt eine Cyberrisiko-Analyse beinhalten müssen. Abschließend wird erörtert, wie sich die Beziehungen zwischen diesen zuvor voneinander getrennten Bereichen nun entwickeln müssen, um das unternehmensweite Modell des Cyberrisiko-Managements zu ermöglichen, das die Boards zunehmend erwarten.





## ÜBER DIE AUTOREN

**Die Internet Security Alliance** ist führend auf dem Gebiet der Cybersicherheit und arbeitet mit der US-Regierung zusammen, um sich für eine öffentliche Politik einzusetzen, die die Interessen der Cybersicherheit fördert.

**Larry Clinton** ist Präsident und CEO der Internet Security Alliance. Er berät Industrie und Regierung in Fragen der Cyberpolitik und tritt regelmäßig in den Medien als Experte auf. Er hat die NATO, die Organisation Amerikanischer Staaten (OAS), die G20 und den US-Kongress instruiert. Zweimal wurde er in die NACD-Liste „Directorship 100“ der einflussreichsten Personen auf dem Gebiet der Corporate Governance aufgenommen.



KAPITEL 1

# CYBERSICHERHEIT IST (NICHT) EIN IT-PROBLEM

VON LARRY CLINTON, PRÄSIDENT UND  
GESCHÄFTSFÜHRER DER INTERNET SECURITY  
ALLIANCE, UND CARTER ZHENG,  
FORSCHUNGSMITARBEITER DER ISA

