CONTENTS

About the author viii
List of contributors ix
Preface x
Acknowledgements xiii

PART ONE Contextualizing cybersecurity risk

01 **Why now? The only constant is change** 3

Digital transformation and the relevance of a digital strategy 5
Characteristics of a disruptive company 11
References 28

02 **Technologies and security challenges** 32

The security of new technologies 33
Data science 51
References 68

03 **Data breaches** 73

Important breaches 74
Breach response 92
References 94

PART TWO Cybersecurity programme management

04 **What are cybersecurity and cybercrime?** 101

Cybersecurity backdrop 102
Cyber-attacks, attribution and cybersecurity 112
References 135

05 **Establishing a cybersecurity programme** 141

The security function 143
The cyber programme structure and objectives 163
References 179

PART THREE Actors, events and vulnerabilities

06 **Threat actors** 183

Actor DNA 185
The CIA triad and actor objectives 189
Threat actor attributes 200
Motivations for threat actors 211
References 222

07 **Threat events** 227

Threat event DNA 227
Malicious threat events 235
Accidental threat events 254
Threat modelling 256
References 269

08 **Vulnerabilities** 272

Vulnerabilities in technology 273
Vulnerabilities in people 299
Vulnerabilities in process 303
Finding vulnerabilities: security testing and assurance 306
References 313

09 **Controls** 317

What is a control? 318
Common controls: people 330
Common controls: process 335
Common controls: technology 350
References 364

PART FOUR Conclusion: the cybersecurity risk equation explained

10 **Cyber risk management: a conclusion** 369

What is risk? 370
Performing a risk assessment 384
Risk frameworks 402
Information classification 416
References 422

Index 424