Cyber Security: Law and Guidance

Second Edition

Helen Wong MBE

BLOOMSBURY

Contents

About this Book v
Dedication viii
Contributors ix
Table of Statutes xli
Table of Statutory Instruments xlv
Table of Cases xlvii

1. THREATS 1
By Helen Wong MBE

What are Cyber Security Threats? 1
Who are the Perpetrators? 4
States and state-sponsored threats 4
Terrorists 5
Hackivists 5
'Script kiddies' 6
Examples of Threats 6

2. VULNERABILITIES 9
By Helen Wong MBE

What are Cybersecurity Vulnerabilities? 9
What are Flaws? 9
Cybersecurity Vulnerability Vs Ccyber Threat: What's the Difference? 9
Four Vulnerabilities 10
How to Stay Protected Against Cybersecurity Vulnerabilities 12
An Expanding Range of Devices (Internet of Things) 14
Poor Cyber Hygiene and Compliance 14
Insufficient Training and Skills 15
Legacy And Unpatched Systems 15
A Validation Process 16
Implementing this Guidance 16
Wider Organisational Relevance 16
Different Types of Update 16
Rolling out Testing 17
Best-Practice Timescales 18
Updating when Exploitation is Rife 18
Asset Discovery 19
Outdated and Products with Extended Support 19
Configuration Management 20
Carry out Assessments by Triaging and Prioritising 20
Scanning 21
Vulnerability Disclosure 21
Choosing not to Update 21
Verification 23
Regularly Review 24

3. THE LAW 25
By Ria Halme
Introduction 25
International Instruments 25
Convention 108 25
Council of Europe Convention on Cybercrime 27
European and European Union-Level Instruments 28
The Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) 28
European Court of Human Rights (ECtHR) and the application of the ECHR to privacy and data protection 29
Case law of the ECtHR (on privacy and security) 30
Treaty of Lisbon and the EU Charter of Fundamental Rights and Freedoms 31
The EU's General Data Protection Regulation (GDPR) 34
E-privacy Directive 40
Payment Service Directive 2 (PSD2) 41
Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) 45
The Directive on security of network and information systems (NIS Directive) and NIS2 47
Uk's Legislation 50
The UK's Human Rights Act 1998 (HRA) 50
UK GDPR and the Data Protection Act (2018) 53
The Privacy and Electronic Communications (EC Directive) Regulations (PECR) 56
Regulation of Investigatory Powers Act (RIPA, 2000), Data Retention and Regulation of Investigatory Powers Act (DRIPA, 2014), Investigatory Powers Act (IPA, 2016) 56
Computer Misuse Act (CMA) 58
CMA in practice 59
A Focus on the Computer Misuse Act 60
By Gary Broadfield
Territorial Scope 70
Sections 4 and 5 70

4A. THE RISK PRACTITIONER'S JOURNEY: RISK ALIGNED ASSURANCE AND THE THREE LINES OF DEFENCE 77
By Farid Abdelkader
Section 1: An Introduction to Risk Aligned Assurance and my Journey across the Three Lines of Defence 77
Section 2: The Beginning – OCC's CFR 12 Part 30, Global Regulations, and The Three Lines of Defence 78
Section 3: Risk Aligned Assurance – The Evolution of The Three Lines of Defence and the Emergence of Aligned Assurance 79
Section 4: Risk Aligned Assurance and its Leverage across Industries 80

Section 5: Case Studies – The Benefits Of Aligned Assurance 81
Section 6: Implementing Risk Aligned Assurance – Key considerations and Best Practices 83
Section 7: Managing, Monitoring, and Reporting on Risk Aligned Assurance to Senior Management and the Board of Directors 85
1. Roles and Responsibilities: The RACI Model 85
2. Risk Appetite 85
3. Key Metrics 85
Section 8: The Crucial Role of Risk Aligned Assurance: The Executive Stakeholders, Shareholders, and Policy Holders Lens 86
Section 9: The Future of Risk Aligned Assurance 88
Section 10: Essential Skills for Risk Practitioners in the Era of Risk Aligned Assurance 89
Section 11: Epilogue – The Ongoing Journey of Risk Aligned Assurance and the Role of Professional Associations and Standard-Setting Bodies 90
Section 12: Trust, Collaboration, Teaming, and Transparency in Risk Aligned Assurance 91
Section 13: Conclusion – Embracing the Future of Risk Aligned Assurance 92

4B. DEFEND BY NATIONAL CYBER SECURITY CENTRE 95
NCSC Research Problem Book – How to Defend 95
The NCSC research problem book 95
Introducing the problem book 95
Who is it For? 95
How Should it be Used? 96
The Chapters 96
The cross-cutting problems 96
The hardware security problems 96
Cross Cutting Problems 96
Strands or sub-problems 97
How do we Make System Security Assessments more Data Driven? 99
Strands or sub-problems 99
How do we Create and Adopt Meaningful Measures of Cyber Security? 101
Strands or sub-problems 101
How do we Make Phishing a Thing of the Past? 102
Strands or sub-problems 102
How can we Accelerate the Adoption of Modern Security Mitigations into Operational Technology? 103
Strands or sub-problems 103
Introducing the hardware security problems 105
What do we Mean by Hardware Security? 106
Strands or sub-problems 107
How do we know that we can Trust our Devices? 108
Strands or sub-problems 108
Which Device Architectures help us Improve Security Further up

the Stack? 109
Strands or sub-problems 109
How do we Integrate Secure Devices so they Contribute to Security at the System Level? 110
Strands or sub-problems 110

5. PRIVACY AND SECURITY IN THE WORKPLACE 113
By Ria Halme
Introduction 113
Legal Instruments on Data Protection and Security in the Workplace 113
Role of the Employer 115
The definition of an employee 115
Categories of Personal Data Processed in the Employment Context 115
Legal grounds for processing personal data 116
Data Protection and Security Requirements Extend to all Medias 116
The Controller is Responsible for Choosing a Compliant Data Processor 117
Roles of the Controller and the Processor 117
Training and Awareness 120
Privacy Matters, even in Data Security 122
Identity and Access Management (IAM) – Limit Access to Data 124
Remote Workers 125
Data Subject's Rights 127

6. CYBER SECURITY AND PHYSICAL BUILDINGS 129
By Helen Wong MBE
Information Technology (IT) and Operational Technology (OT) 129
Connected and Smart Buildings 131
Digital Engineering and Built Asset Information 132
Security of Endpoints 132
Information Management 133
Cyber Security 133
Security Goals 134
Security Principles 135
Security goals for cyber-physical systems 136
Managing Change 137
The Built Asset Lifecycle 137
Applying Cyber Security Through the Lifecycle of a Built Asset 138
Who is Accountable and Responsible for the Cyber Security of Built Asset Systems and Data? 139
Strategic level 139
Operational level 139
What Built Asset Systems and Information Assets need to be Protected? 139
What Could Adversely Affect the Built Asset Systems and Data? 141
Where are the Built Asset Systems and Data Located? 142
How Should Built Asset Systems and Data be Protected? 143

7. CYBER BREACH PLAYBOOK 145
By Helen Wong MBE
Introduction 145
Overview 145
Purpose 145
Malware Definition 146
Scope 146
Review Cycle 146
Preparation Phase 146
Detect 148
Analyse 151
Remediation – Contain, Eradicate and Recover 153
Post Incident 155
Annex A: Flow Diagram 157

8. THE C SUITE PERSPECTIVE ON CYBER RISK 159
By Klaus Julisch
Organisational Ramifications of Cyber Risk 159
Assigning Accountability 160
Setting Budgets 162
Building a CXO-led Cyber Strategy 163
Summary and Outlook 166

9A. CHECKLIST FOR ADDRESSING AND PREPARING FOR CYBERSECURITY INCIDENTS 169
By Helen Wong MBE
Action Items 169

9B. CYBER INCIDENT CHECKLIST 177
Appendix 180
Triage Questions 180

9C. SECURITY INCIDENT NOTIFICATION REQUIREMENTS (UK) 183
Overview 183
Types of Incidents Covered 183
Notification Obligations 183
Specific Notifications 184
Personal Data Breaches (UK GDPR) 184
Telecommunication Networks and Service Providers (PECR & CA 2003) 185
Operators of Essential Services (NIS Regulations) 188
Trust Service Providers (UK eIDAS) 190
Regulated Financial Institutions (FCA & PRA) 192
Pension Schemes (Pensions Act 2004) 192

10. INDUSTRY SPECIALIST IN-DEPTH REPORTS 193

10A. MOBILE PAYMENTS 193
By Rhiannon Lewis

Key Technical and Commercial Characteristics of Mobile Payments 193
Complex Regulatory Landscape 194
Key Technical Characteristics of Authentication 195
Key Commercial Characteristics of Mobile Payment Authentication 196
Information Security Risks of Mobile Payments to Consumers 196
Information Security Risks of Mobile Payments to the Payment System 198
Legislative Framework Governing Payment Authentication in Europe 199
Regulation of Strong Consumer Authentication 202
Other Sources of EU Guidance 203
Legislative Framework Governing Payment Authentication in the United States 203
Industry Standards Governing Payment Authentication do not Exist in the Context of Mobile Payments 204
Competition Law and Mobile Payments 205
Conclusion 206

10B. ELECTRIC UTILITIES: CRITICAL INFRASTRUCTURE PROTECTION AND RELIABILITY STANDARDS 206
By E Rudina and S Kort

Electric Utilities as a Part of Critical Infrastructure 207
Electric Utilities as a Kind of Industrial Automation and Control System 207
Current State and Further Evolution of Electricity Infrastructure – Smart Grid 208
Sources of Cybersecurity Issues for Electric Power Infrastructure 209
Known Cyberattacks on Electric Utilities 210
Why Guidelines and Standards for the Protection of Electric Utilities Matter 216
The Recommended Practice: Improving Industrial Control System Cybersecurity with Defence-In-Depth Strategies By ICS-CERT of the US Department of Homeland Security 217
The Electricity Subsector Cyber-Security Risk Management Process by the US Department of Energy 219
The NERC Critical Infrastructure Protection Cybersecurity Standards 220
The ISA99/IEC 62443 Series of Standards for Industrial Automation and Control Systems Security 226
Cyber-Security Capability Maturity Model (C2M2) by the US Department of Energy 229
Critical Infrastructure Cybersecurity Framework by the US NIST and Implementation Guidance for the Energy Sector 231
UK National Cyber Security Centre Guidance Documents 233
NIS2 Directive 236
Specific Cybersecurity Considerations for the Nuclear Power Plants 237

10C. SECURING CRITICAL MANUFACTURING SECTORS FROM MODERN CYBER THREATS 239
By Helen Wong MBE

Introduction to Critical Manufacturing 239
Defining Critical Manufacturing and its Future Trajectory 240
Industry 4.0: Evolution and Components 240
Robotics 240
Wearables 240
3-D Printing 240
Internet of Things/Industrial Internet of Things (IoT/IIoT) 241
Virtual Reality/Augmented Reality (VR/AR) 241
Machine Learning/Artificial Intelligence (ML/AI) 242
Big Data Analytics 242
5G 242
Framework for Industry 4.0 243
Deploying Industry 4.0 Technologies 243
Cybersecurity in Manufacturing 244
IT vs. OT Cybersecurity 244
Rising Cyber Threats in Manufacturing 244
Main OT Threat Actors and Attack Examples 245
Enhancing OT Cybersecurity 245
Conclusion 246
247

10D. UK FINANCIAL SERVICES 248
By Steven Peacock

Introduction 248
How Severe Could the Impact of a Cyber-Attack Be? 249
How Should Organisations Tackle the Challenge of Cyber Attacks? 249
Regulator Focus Within the UK 253
Other Threats and Challenges Facing Retail Banking 254
Appendix 1 255
References 256

10E. CYBERSECURITY FOR THE ENERGY SECTOR: TOWARD ENERGY 4.0 257
By Stefano Bracco

The Energy Sector: Moving to the Age of Smart and Digitalised Markets 257
Critical Infrastructures in Energy and their Key Role for the Civil Society 259
The IT-OT Dilemma 260
The Legal Efforts in the US 262
The Ukrainian Case 265
The Legal Developments in the European Union 267
An Analysis of the Energy Sub Sectors: Strengths, Weaknesses and Law 278
Conclusions and the Way Forward 284

10F. AEROSPACE, DEFENCE AND SECURITY SECTOR 285
By Simon Goldsmith
Introduction 285
Comparing Civilian and Military Cyber Security Sectors 286
The Digital Age and the Digital Battlespace 287
Offensive Cyber Capability 287
Criminal Malware Development 290
Benefit and Threat 290
Opportunities for the ADS Sector 291
Evolution of the Threat 291
Corporations on the Frontline 293
Example of Proliferation – Stuxnet 293
Payload 294
A New Weapon 296
Example of Civilian Infrastructure Under Attack – Ukraine Power Grid 297
Wider Concerns 298
Example of Criminal Attacks at Scale – Swift Payment Network 298
Performance of the ADS Sector in Cyber Security 302
Notable Cyber Security Events in the ADS Sector 310
Cyber Security In Non-Government Sectors: Missed Opportunity? 312

10G. BANKING IN THE EMIRATES – THE NBD WAY 313
By Yazad Khandhadia
The People: Building a Solid Team 313
The Process: Building a Program 316
The Technology: Oh! The Gadgets! 319
In Closing 323

10H. HEALTHCARE 324
By Helen Wong MBE
Introduction 324
What is Wannacry? 325
What is Ransomware? 325
How the Department and the NHS Responded 327
Key Findings 330
Practical Points: Prevention and Protection 331
Selling or Buying your Healthcare Practice – Things to Look out For in the Due Diligence 333

10I. MEDICAL DEVICES 334
By Helen Wong MBE
Introduction 334
Conclusions and Recommendations 341

11. SOCIAL MEDIA AND CYBER SECURITY 343
By Helen Wong MBE
Introduction 343

Why Social Media is Vulnerable to Cybercrime 343
Increased Risk of Social Engineering Attacks 343
Oversharing 344
Data Aggregation 344
Unsecured Portable Devices 345
Business Cyber Risks Associated with Social Media 345
Social Media Poses Significant Cybersecurity Risks for Businesses, such as Social Engineering, Identity Theft, and the Spread Of Malware 346
How to Reduce the Cyber Risks of Social Media Use 346
Social Media Access Control 346
Social Media Policy Implementation 347
A Checklist for Companies Using Social Media 347
Establish terms of use and privacy policies 347
Determining the applicability of defences under 348
Prepare take down policies and procedures 348
Incorporating third-party websites for business purposes 348
The rules governing promotions and competitions 349
Consider Using Social Media as a Legal Tool 350
Possibility of Market Manipulation 350
Reflect on the Legal Risks Involved in Using Social Media for Screening Purposes 351
Mentions of the Company on Related Social Media Platforms 352
Insurance 352
In Summary 353
Social Media Checklist for Employees 353
There has been a breach of the terms of employment 354
Train Employees 353
In Summary 355
What is Social Media and Why Does it Matter? 356
Social media classifications 356
Widely Used Social Media Sites and Services 356
Here is an example of a social media policy 359

12. INTERNATIONAL LAW AND INTERACTION BETWEEN STATES 363
By Benjamin Ang and Tan E-Reng
Determining if International Humanitarian Law / Law of Armed Conflict Applies 363
Applying Principles of IHL and LOAC 366
NATO Responses 367
United Nations Charter Responses 368
Use of force 368
Armed Attack and Right of Self-Defence 368
Non-State Actors 369
Cyber Norms as the Basis for International Law 370
UNGGE Cyber Norms 370
The Future for Cyber Norms 375
Interaction Between States 375

International Challenges of Cyber-Crime 376
Criminalising Transnational Cyber-Crime 376
Conventions, Treaties and Mutual Legal Assistance 377
Limitations to Mutual Legal Assistance 379
Case Study: Singapore's Interactions with other States on Cyber-Issues 379
Cooperation in Fighting Cybercrime 379
Cooperation in Joint Activities Between ASEAN Member States 380
Cooperation Through Memoranda of Understanding 381
Cooperation in Developing International and Regional Norms 381
Creating the Need for Cooperation Through National Legislation 382
The Future of International Law and Interaction Between States in Cyberspace 383

13. SECURITY CONCERNS WITH THE INTERNET OF THINGS 384
By Kevin Curran

Introduction 387
How Organisations can Secure IoT 387
Industry-Wide Initiatives for IoT Security 391
Future IoT Innovations 393
Future Short-Term Challenges 394
Conclusion 396
397

14. MANAGING CYBER-SECURITY IN AN INTERNATIONAL FINANCIAL INSTITUTION 399
By Cosimo Pacciani

The Liquid Enemy: Managing Cyber-Risks in a Financial Institution 399
The Liquid Enemy 399
Foreword 399
Cyber risk, the liquid enemy 400
Coding a Financial Institution Approach to Cyber-Risks 402
Three lines of defence and Cyber-risks 402
Key building blocks for managing cyber risks 408
Riding the Waves: Some Points for a New Approach to Risk Management of Cyber-Security 414
Definition of 'cyber-risk' as stand-alone category 414
Cyber Risk Appetite 416
Deep and Dark webs: Alice's mirrors 417
Personal data protection issues 418
Conclusion: Cyber-Risks in an era of AI Continuity 419

15. EMPLOYEE LIABILITY AND PROTECTION 423
By Sally Penni

Overview and Introduction of the Problem 423
Why do employees take the information? 423
What Information is Confidential? 424
What is confidential information? 424
What Information will the Courts Protect? 425

Advice 427
Employer beware 427
Employer beware 427
Breach of confidence cases 428
Employer beware 428
Trade secrets 429
What Protection Does the EU Offer on Trade Secrets? 429
The Trade Secret Directive 2013 429
The Trade Secrets Directive in short 429
What is Copyright? 431
Uk Law and the Copyright, Designs and Patents Act 1988 431
What are the Categories of Protection in UK Law? 431
Employer beware 432
What Does the Caselaw Offer by way of Protection on Copyright? 432
The EU and the Software Directive 433
What is the Definition of the Functionality of Computer Programs Within the Software Directive? 434
What Protection is There if the Program was Created by the Employee Acting in the Performance of his Duties? 434
What is Permitted Under the Software Directive? 434
Advice 435
What Protection is Offered to Databases? 435
What is a database? 435
Issues with a database? 435
What Protection of Databases is Available From EU Directives? 436
Is There any Protection of Databases to Protect Software? 437
The Facts 437
Navitaire v Aasyjet 437
Facts 437
Held 438
What do These Cases Teach about Protection from Employees? 438
Advice 438
Employers' Liability 439
What is Being Directly Liable and can the Employer be Vicariously Liable for the Conduct of an ex Employee? 439
What is direct liability? 439
When does direct liability arise? 440
What is vicarious liability? 440
VL and harassment 441
And discrimination under the Equality Act 2010 441
VL and internet usage 441
Directors' Liability for Breach of Confidence 442
In What Ways can a Directors Liability be Imposed? 442
What Measures, Systems and Procedures are Sufficient to Avoid Employer Liability? 443
Contracts of Employment as a Means of Protection 444
Notices 445
Training employees 445

Disciplinaries as a means of protection 445
Conclusion 446

16. DATA SECURITY – THE NEW OIL **447**
By Ryan Mackie

Data Security in an Age When Data is The New Oil 447
UK ICO Data Security Incident Trends 448
Data Security Verses Information Security Verses Cyber-Security 450
Data Security Verses Information Security 450
Information Security ('InfoSec') Verses Cyber-Security 450
UK Data Security Law 451
Civil Law 451
UK General Data Protection Regulation ('UK GDPR') and Data Protection Act 2018 ('DPA 18') 452
UK GDPR 453
The DPA 18 453
UK General Data Protection Regulation ('UK GDPR') and EU General Data Protection Regulation ('EU GDPR') 454
The Data Protection Act 2018 ('DPA 18') 457
UK Privacy and Electronic Communications Regulations 2003 ('PERC') 458
The Privacy and Electronic Communications Directive 2002/58/Ec (the 'Eprivacy Directive') and The Proposed 'Eprivacy Regulation' 459
Criminal Law 460
Cyber-crime 460
UK Criminal Law 461
Cyber-Dependent Crimes 462
Cyber-Dependent Crimes – Offences and Legislation 462
Computer Misuse Act 1990 (CMA) 462
Regulation of Investigatory Powers Act (RIPA) 2000 464
Investigatory Powers Act 2016 (IPA) 465
Data Protection Act 2018 (DPA 18) 466
Crimes Introduced Under the DPA 2018 466
Cyber-Enabled Crimes 467
Cyber-Dependent Crimes – Offences and Legislation 468
Fraud 468
The Fraud Act 2006 (Fraud Act) 469
The Theft Act 1968 470
Conclusion 470

17. DATA CLASSIFICATION **473**
By Dr Reza Alavi

Introduction 473
What is Data? 473
Data Classification 474
The Benefit of the Data Classification 474

Data Classification Process 476
Data Classification: A Practical Example 477
Challenges of Data Classification 479
The Ramification of Failure ofData Classification Scheme 479
Data Classification and Business Impact Analysis (BIA) 480
A Keys to a Robust Data Classification Strategy 481
Data Privacy and Security 482
What is Data Security? 482
What is Privacy? 482
Why is Data Security Mistaken for Privacy? 483
Types of Controls 483
Asset Discovery 485
Asset Visibility Strategies 485
Asset Classifications 486
Automated Asset Management 486
Data Loss Prevention (DLP) 486
Conclusion and Future Outlook 488

18. LIABILITY FOLLOWING A DATA BREACH **489**
By Mark Deem and Adelaide Lopez

Liability Issues Following a Cyber-Attack 489
The Liability Landscape 490
Technology 490
Threat Actors 491
Evolution of Threats 491
How threat vectors manifest themselves as a potential liability 492

19. CRIMINAL LAW **507**
By Jill Lorimer and William Christopher

Introduction 507
Misuse of Computers 507
Unauthorised access to computer material – section 1 offence 508
Unauthorised access with intent to commit or facilitate commission of further offences – section 2 offence 509
Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc – section 3 offence 509
Unauthorised acts causing, or creating risk of, serious damage – section 3ZA offence 510
Making, supplying or obtaining articles for use in computer misuse offences under section 1, 3 or 3ZA – section 3A offence 511
Jurisdictional issues 512
Review of the 1990 Act 512
Malicious Communication and Harassment 513
Malicious and offensive communications 513
Cyber-stalking and harassment 515
Trolling 516

Revenge porn 517
Sending of Explicit Images 518
Indecent and Obscene Material 518
Obscene publications and extreme pornography 519
Indecent images of children 522
Data Breaches 524
Data Protection Act 1998 524
Data Protection Act 2018 524
Enforcement 525
Criminal offences 525
Defences – section 170(2) and (3) 526
Sentencing 527
Fraud 527
Fraud Act 2006 528
Variants of cyber-fraud 529
Crypto asset and Initial Coin Offering fraud 532
The Civil Perspective 534
Banks 539
Crypto Assets 545

20. THE DIGITAL NEXT WAY 549
By Mark Blackhurst

Cyber Attacks 549
Protecting your Business 550
GDPR 551
Steps to Update your Online Security 552
Employee Safety 554
Protecting your Remote Workforce 555

21A. PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE ACT 2022 (THE ACT) 557
By Helen Wong MBE

Overview 557
Background 557
Purpose and Structure of the Act 557
Applicability and Scope 558
Key Obligations 558
Compliance with Security Standards 559
Statement of Compliance 559
Addressing non-Compliance 559
Enforcement Mechanisms 559
EU/UK Context 560
Practical Implications for Businesses 560
Conclusion 560

21B. INTELLIGENCE AND THE MONITORING OF EVERYDAY LIFE 561
By Dr Victoria Wang and Professor John V. Tucker

Introduction 561

Background 562
Surveillance as the Monitoring of Everyday Life 565
Established Surveillance Technologies 565
Technologies of Daily Life 567
Perfect Surveillance 569
Digital Intelligence 570
Privacy and Identity in Digital Intelligence 575
On Privacy and Identity 575
On Digital Privacy 577
Theorising Identity 578
On Identifiers 579
Some Observations on Identifiers 581
Conclusion 583

22. CYBER SECURITY LAW AND LEGISLATION: PROTECTING DATA IN THE UK, EU, AND USA: BREACHLESS LIABILITY 585
By David Clarke

Introduction 585
Importance of Cyber Security Law 585
Breachless Liability 585
Scope of this Chapter 586
Top 21 Cyber Security and Data Security Measures to Assist in Breachless Liability 586
Ensure Executive Alignment 588
Continuous Security Improvement 589
Organisational Cyber Commitment 590
Legal Breach Consultation 590
Urgent Security Patching 590
Executive Cybersecurity Updates 591
Monitor for Data Loss 591
Web Usage Filtering 591
Scalable Backup Systems 591
Apply Least Privilege Principle 592
Manage Unused Account Risks 592
Control Organisational Communications 592
Offline Insurance Contact List 593
Standardise Endpoint Security 593
Robust MFA Utilisation 594
ZTNA for Secure Access 594
XDR Strategy Implementation 594
Records Management Security 594
Cybersecurity Strategies 595
Asset Classification Process 595
Systematic IAR Setup 595
Key Legislation for Data Breaches and Breachless Liability 596
UK Data Protection Act 2018 Fines 596
UK Network and Information Systems (NIS) Regulations 2018 596
Telecommunications (Security) Act 2021 596

USA (Virginia) Consumer Data Protection Act (CDPA) 597
USA (Colorado) Colorado Privacy Act 597
USA (Nevada) SB 220 597
USA (Maine) LD 946 598
USA (New York) SHIELD Act 598
USA (California) California Consumer Privacy Act (CCPA) 598
China Data Security Law of the People's Republic of China 598
EU Digital Operational Resilience Act (DORA) 598
EU Cybersecurity Act 599
EU Network and Information Systems Directive (NIS Directive) 599
EU General Data Protection Regulation (GDPR) 599
USA Health Insurance Portability and Accountability Act (HIPAA) 599
USA Gramm-Leach-Bliley Act (GLBA) Fines 600
USA Cybersecurity Information Sharing Act (CISA) 600
India Personal Data Protection Bill 2022 600
India Information Technology Amendment Act 2018 600
UK Online Safety Bill 2023 Fines, regulatory action 601
UK Network and Information Systems (NIS2) Directive 601
Data Breaches and Legal Consequences 601
Summary of Unauthorised data sharing, breach and transparency issues 601
Non-Compliance with Cybersecurity Regulations 602
Inadequate Incident Reporting and Remediation 602
Risks of Harmful Online Content 602
Unauthorised Access and Data Tampering 602
Failure to Report Data Breaches 603
Non-Compliance with Encryption Standards 603
Cross-Border Data Transfer non-Compliance 603
Consumer Rights and Data Selling Issues 603
Future Trends and Challenges in Cyber Security 604
Numbered Checklist Summarising the Cyber Security/Data Protection Recommendations 604
Conclusion 605
Importance of Compliance with Cyber Security Law 605

23. DATA ARCHITECTURE: CYBERSECURITY'S SILENT PARTNER 607
By Kevin Murphy

Abstract 607
Data and Attack Vectors: Re-Interpreting the Threat Landscape 607
Ransomware 608
Supply Chain 609
Insider Risk 610
Primacy of 'Identity' Data Points 611
Historical Challenge of Managing Identity: Complexity 611
To Protect, First Modernise 611
Identity: Risk Beyond IT – Ensuring Business Engagement 612
Modernising the IAM Estate: An Emerging Architecture 612

Zero Trust Architecture 613
ZTA Foundations 614
ZTA Performance: Secure the Data Plane 614
How ZTA Informs Cybersecurity Data Architecture 615
From Data Points to 'Profiles': Emerging IAM Data Architecture 616
Beyond Identity: IAM Data Architecture to Ubiquitous Visibility Across the Cyber Risk Profile 616
Security Operations: Identity Profiles and the Foundations of a New Data Architecture 617
Scale of IAM Threats: Detecting Compromise 617
Re-imagining Security Operations – Historic Challenge 617
Danger of a Myopic Architecture 618
The Silent Partner: Data Driven Security Architecture 618
Taming Volume 619
The 'Silent Partnership': Foundations of Data Good Practice 620
From Data Engineering to Data Science 621
Enhancing SOC Performance 621
Assuring Cybersecurity Data Sources 622
Beyond Security: Predictive Analytics and Automated Interventions 623
Profiling: From Data to People 623
Talent Shortfall 623
Business Agility: Devolved Cyber Decision-Making 623
Cyber Skill Development: A Strategic View 624
Retaining Cyber Talent 625
Cyber Skill & User Experience: Return on Investment 626
Risk Management 626
Data Fabric Enabling Continuous Risk Assessment 626
An Agile Data Architecture: Supporting Risk Decision Making 627
Composable Security Requires Composable Data 628
Bringing it All Together: Cybersecurity Strategy – Pathway to Supporting the Data-Led Era 629
Core Components 629
Common Strategic Limitations 629
New Approach: First Principles 630
Agile Strategy 630
Strategic Inter-dependencies: Technology, User Experience, & Data 631
Modernisation & Simplification: Factoring the Legacy Estate 631
User Experience is a Cybersecurity Strategic Imperative 632
Data: Protecting & Leveraging 632
Moving Forward 632

24. MERGERS AND ACQUISITIONS CORPORATE DUE DILIGENCE AND CYBER SECURITY ISSUES 635
By Vijay Rathour

The Sins of our Fathers 635

The 'New Oil' 637
Un-Due Diligence? 639
Warranty and Indemnity Insurance 641
The Observer Effect 641
Oiling the Supply Chain 643
Morrisons and the Disgruntled Insider 643
Conclusions 644

25. PROTECTING ORGANISATIONS **645**
By Gary Hibberd

Introduction 645
The UK's National Cyber Security Strategy 645
Standard Practice 646
PCI DSS 647
Cyber Essentials and Cyber Essentials Plus 650
How Cyber Essentials protects your organisation 651
The Certification Process 652
Cyber Essentials Plus 652
The problem(s) with Cyber Essentials 653
Benefits of Cyber Essentials 654
ISO27001:2022 654
ISO27001 & ISO27002 655
Context of the organisation 656
Leadership 656
Planning 657
Support 657
Operation 658
Performance evaluation 658
Improvement 658
Annex A Controls 659
Conclusion 659

26. PUBLIC PRIVATE PARTNERSHIPS **661**
By E Rudina

Introduction 661

27. CYBERSECURITY DISPUTES **667**
By Ffion Flockhart, Charlie Weston-Simons and Steven Hadwin, Allen Overy Shearman Sterling LLP

Introduction 667
Personal Data Breach Claims 669
Commercial Disputes 678
Background 678
Elements of a typical Customer/Victim contractual dispute 679
Other commercial disputes 683
BEC Disputes 684
Injunctions 685

Insurance Claims 686
Appeals of ICO Notices 687

28. THE JELLO PROBLEM: KEY FEATURES OF GENERATIVE AI THAT CREATE LEGAL RISK **689**
By David Wakeling and Marcus Turner

Introduction 689
Scope 691
AI-Specific Regulation: A Risk-Based Approach? 693
EU AI Act 693
UK White Paper 695
US Presidential Executive Order 695
General Litigation Risk 696
Disputes with customers 696
Disputes with third parties 698
Disputes with foundation model providers 699
Overview of Data Risks 700
Factors affecting data risk 701
Transparency 701
Transparency and the GDPR 702
Transparency and the EU AI Act 703
Transparency and US law 704
Transparency obligations in practice 704
Types of explainability 706
Fairness and Bias 707
Fairness, bias and the EU AI Act 708
Fairness and bias during the process 709
Selecting training data: ethical considerations 710
Intellectual Property Infringement Risk 710
Relevant intellectual property rights in training data 711
Factors affecting the copyright infringement risk 712
Copyright infringement at point of training (and possible exceptions for the developer) 712
Copyright infringement at point of use (and possible exceptions for the user) 714
The results of a finding of infringement 716
Internal Risk 716
Deployer's intellectual property inserted as a prompt 716
Copyleft code in output 717
Ownership Risk 718
Subsistence of copyright in AI-generated works 718
Ownership of copyright in AI-generated works 718
AI-generated inventions and patents 719
Risk Management Framework: The Three Risk Management Pillars 720
Use Case + 720
Operational 721
Contractual 721
Conclusion 721

29. CYBER SECRET, LIFE SECRETS – ON THE VERGE OF HUMAN SCIENCE 723
By Arthur Keleti
Introduction 723
Shades of Secrets 724
Privacy 726
Data Breaches 730
The Risk Paralysis 731
And Then There Were Bugs 733
Mass Surveillance 734
The Post-Snowden World 737
The World of Untrust 740
AI is the New Authentic? 742
What's the Solution? 743

30. A PLAN FOR THE SME 745
By William McBorrough
Building a Small Business Security Risk Management Plan 745
Where do you start? 745
You are not a big, well known business. Why would anyone attack you? 746
It's too costly 746
Hasn't the IT guy(s) already dealt with this issue? 747
Too Complicated? 747
Why you need a formal security program? 748
Current state of security management 748
Security Program Standards and Best Practices 749
Security Program Components 749
It's really all about risks 750
Case Study 750
Security Risk Management Process 751

31. CONCLUSION 757
By Helen Wong MBE
Artificial Intelligence (AI) 757
Industrial Strategy and R&D 758
Data and Online Safety 758
Cyber Security 759
Clean Energy 759
Broadband and 5G 759
How does the Labour Manifesto impact the Cyber Security Space? 759
Prevention is Better Than Cure 761
Internet of Things Will Cause More Cyber-Attacks and Financial Loss. 761
The Rise in Ransomware 761
To Cloud or Not? 762
Can Artificial Intelligence Fight Back? 762

APPENDIX 1: THERESA MAY SPEECH, MUNICH SECURITY CONFERENCE, FEBRUARY 2018 763

APPENDIX 2: CYBERSECURITY LEXICON FOR CONVERGED SYSTEMS 771

APPENDIX 3: THE GOVERNMENT'S NATIONAL RESPONSE 775

APPENDIX 4: SAMPLE LEGAL DOCUMENTS 777

INDEX 795

of behaviour suggests that individuals risk criminal liability for trivial acts, in practice common sense and the limited resources of investigators and the CPS mitigate against that risk. Thus the flexibility of the Act has been a strength, allowing it to remain robust in the decades since it was enacted. In that context it is perhaps less surprising than it may seem at first sight that there is, and never has been, any definition within the Act of the meaning of the word 'computer,' and it is left for the courts of the day to determine what that term may or may not cover.

3.115 In relation to the section 1 offence, section1(1), A person is guilty of an offence if:

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer or to enable any such access to be secured;

(b) the access he intends to secure or to enable to be secured, is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

3.116 Furthermore, section 1(2) further clarifies the position in respect of *mens rea:*

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

3.117 As initially enacted in 1990 the section 1 offence was a summary only offence with a maximum sentence in the Magistrates Court of six months' imprisonment. Section 35(3) of the Police and Justice Act 2006 (PJA 2006) amended section 1 by making the offence triable either way. The PJA 2006 increased the maximum sentence on Summary conviction from six months' imprisonment to two years and stipulated that the maximum sentence available to a Crown Court Judge would be two years imprisonment.

(2) Section 2: Unauthorised access with the intent to commit or facilitate further offences.

3.118 The section 2 Offence builds on section 1 by providing that where an individual commits an offence under section 1 with intent to commit or facilitate the commission of further offences by another. Section 2(2) sets out that this section applies to offences:

(a) for which the sentence is fixed by law; or

(b) for which a person who has attained the age of twenty-one years (eighteen in relation to England and Wales) and has no previous

convictions may be sentenced to imprisonment for a term of five years…

3.119 Again, the provision are widely drafted in order to catch a range of actions: section 2(3) confirms that the 'further offence' to be committed does not have to be committed on the same occasion as the unauthorised access offence, but can be committed 'on any future occasion'. Equally section 2(4) states that the section 2 offence can be made out even where 'the facts are such that the commission of the further offence is impossible'.

3.120 Again, the section 2 offence is triable either way and on summary conviction the maximum penalty is imprisonment for 12 months and a fine. However, in a reflection of the increased seriousness of the offence as compared with section 1, and the seriousness of the 'further offences', the maximum penalty available in the Crown Court is five years' imprisonment as well as a fine.

(3) Section 3: unauthorised acts with intent to impair (or with recklessness as to impairing the operation of a computer.

3.121 Section 3 was significantly amended from its original form by the PJA 2006. As originally enacted, to be guilty of a section 3 offence, an individual had to 'do any act which causes the unauthorised modification of the contents of any computer' with intent to impair the operation of a computer, program, the reliability of data or to prevent or hinder access to a program or data held in the computer. The offence carried a maximum penalty of five years' imprisonment on Indictment.

3.122 The amendment of section 3 was necessary; as originally enacted it covered the offences that were foreseen at the time; that is to say an individual who gained unauthorised access to a system and modified the data therein. Modification in this context meant the amendment or deletion of files, or through uploading a virus, malware or other malicious code to a system. Whilst the original section 3 anticipated those actions and was intended to criminalise them, it did not easily cover a newer generation of internet-enabled offences such as Distributed Denial of Service (DDOS) attacks which came to prominence long after 1990.

3.123 DDOS attacks work by overloading a webpage or ISP with 'spam' traffic from an attack server, or in more recent years a 'botnet' of malware infected internet enabled devices. The malicious spam traffic overwhelms the victim's system, causing it to slow significantly or perhaps to crash altogether. It is worth recording that in latter years, this type of attack has become readily available online where users can subscribe to DDOS-for-hire services where an existing infrastructure can be rented to attack a target of choice. Whilst these attacks are certainly capable of impairing the operation of a victim's computer systems, they do not necessarily *modify* them and thus did not fall squarely within section 3 as initially enacted.

3.124 Thus the amended section 3 was extended so that it covered 'any unauthorised act' in relation to a victim's computer rather than simply unauthorised modification. Furthermore in order to be convicted of an offence under section 3 as originally enacted, an individual had to have both the 'requisite intent and the requisite knowledge.' In short, he or she had to intend to cause a modification that would impair the computer etc and know that the modification was unauthorised. As amended, the Act additionally provides that the damage or impairment caused pursuant to section 3 (3) need not be intended but can also be a result of recklessness.

3.125 The widened scope of the section is clear:

3 (1) A person is guilty of an offence if—

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data; or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) 'act' includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

3.126 The amended section 3 offence is also an either way offence, with the maximum penalty on Summary conviction being imprisonment for a term not exceeding 12 months and a fine. In the Crown Court, the PJA 2006 also increased the maximum penalty from five years' imprisonment to ten.

(4) Section 3 ZA, Unauthorised acts causing or creating risk of serious damage.

3.127 Section 3ZA was inserted into the Act by the Serious Crime Act 2015. The new offence was created as the existing provision under which such offending would previously have been prosecuted, section 3, did not carry sufficient penalties, even after the maximum penalty had been raised to 10 years imprisonment following the PJA 2006 where the object or result of a cyber-attack has been to cause damage to critical national infrastructure. Section 3ZA therefore creates such an offence, triable on indictment only, and allowing the Criminal Courts to impose their most severe punishments.

3.128 Again, a core element of the offence is the commission of any unauthorised act in relation to a computer (s 3ZA (1)(a)), which the individual knows, at the time of doing the act, is unauthorised (s 3ZA (1)(b)). However, in order to be guilty under section 3ZA, the act must also cause or create a significant risk of serious damage of a material kind and the person must intend to cause such damage (s 3ZA (1)(c)) or be reckless as to whether such damage is caused (s 3ZA (1)(d)).

3.129 Damage of a 'material kind' is defined in section 3ZA (2) as being:

(a) damage to human welfare in any place;

(b) damage to the environment of any place;

(c) damage to the economy of any country; or

(d) damage to the national security of any country.

3.130 And damage to human welfare is defined by section s3ZA (3) as being damage that causes:

(a) loss to human life;

(b) human illness or injury;

(c) disruption of a supply of money, food, water, energy or fuel;

(d) disruption of a system of communication;

(e) disruption of facilities for transport; or

(f) disruption of services relating to health.

3.131 Subsection (4) provides that it is immaterial for the purposes of subsection (2) whether or not an act causing damaged does so directly (s 3ZA (4)(2)(a)) or is the only or main cause of the damage (s 3ZA (4)(2)(b)).

3.132 Finally, subsection 5 ensures that the ambit of the act is kept as wide as possible, clarifying that for the purposes of section 3ZA:

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) 'act' includes a series of acts;

(c) a reference to a country includes a reference to a territory, and to any place in, or part or region of, a country or territory.

3.133 Pursuant to section 3ZA (6) the offence is indictable only, reflecting its seriousness and will normally carry a maximum sentence of 14 years. However, subsection (7) allows that where a section 3ZA offence has been committed that causes or creates significant risk to human welfare as defined under subsections (3)(a) and (b), (loss to human life or human illness or injury) or serious damage to national security, the potential penalty is increased to life imprisonment.

3.134 The new section 3ZA therefore represents a significant uplift to the powers of law enforcement to deal with the emerging threat of cyber-terrorism and acts that put at risk vital national infrastructure.

3.135 It should be noted that the threat intended to be countered by section 3ZA is real and one that has already manifested itself within the UK. Perhaps the most high profile cyber-attack of 2017 was the WannaCry Ransomware. The scale of the infection was major; within 24 hours of the first infections on 12 May2017, WannaCry was reported to have infected more than 230,000 computers in over 150 countries, affecting a long list of companies and organisations as diverse as Telefonica, Renault, Deutsche Bahn FedEx, Nissan Hitachi, Sberbank, Petrobras and the Russian Central Bank. By the now familiar method of encrypting infected computers and demanding a ransom in Bitcoin in exchange for the decryption keys, the attack caused widespread disruption to systems around the world.

3.136 Crucially, a number of NHS trusts throughout the UK were also affected; according to the National Audit Office, the attack led to disruption in at least 34% of trusts in England (81 out of 236). A further 603 primary care and other NHS organisations were infected by WannaCry, including 595 GP practices. The effect was that thousands of appointments and operations were cancelled. In five areas accident and emergency departments were unable to treat some patients leading to them being diverted further afield.[231]

3.137 It is easy to see how the creators of the WannaCry pathogen would fall squarely within the new section 3ZA. Malware, and particularly Ransomware like WannaCry are indiscriminate in nature, they spread automatically and infect wherever possible. However, whilst the intention of the creators of WannaCry was more likely to be the harvesting of ransom monies rather than to deliberately cause disruption to critical infrastructure, the effect of WannaCry in practise

231 www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

was certainly to cause the 'disruption of services relating to health' and 'risk of causing loss to human life, illness and injury'. In releasing code of this nature 'into the wild' the creators were certainly reckless as to the consequences.

3.138 However, although section 3ZA may put in place the legal framework to fully deal with this type of offending, it may well be the case that section 3ZA is only ever rarely used by the authorities; hacking threats of this nature would seem to largely derive from Nation States (WannaCry was suspected to be a tool created by North Korea)[232] or terrorist groups operating extraterritorially where practical difficulties in respect of investigation may preclude a prosecution. As yet, it is unclear whether any prosecutions have been brought under this provision.

3.139 Alternatively, it may be that as the provision is so widely drafted, in future years section 3ZA becomes used more regularly in cases not involving the above groups. One potential example where it might be considered would be in relation to hacking or computer misuse linked to 'swatting' which can cause widespread disruption and risk to life (in respect of which see **Chapter 1.17** 'Script Kiddies'), although that would seem to diverge somewhat from the original intention behind the provision.

(5) Section 3A: Making, supplying or obtaining articles for use in offences under section 1, 3 or 3ZA

3.140 Section 3A was added to the Act by the PJA 2006, in response to the growing market for 'hacking tools' that were becoming widely disseminated online.

3.141 The offence itself is relatively straightforward; a person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3Z, (s 3A (1)) or if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA (s 3A (2)). Equally an offence is made out if an individual obtains any article intending to use it to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA, (s 3A (3)(a)) or with a view to its being supplied for use to commit, or to assist in the commission of, those offences (s 3A (3)(b)).

3.142 Section 3A (4) specifically confirms that an 'article' includes any program or data held in electronic form, thus ensuring that it encompasses software programs and tools commonly used for fraud and computer crime, such as Remote Access Trojans that, if uploaded to a victim's system (usually through a successful phishing scam) will allow the attacker to take control of it.

3.143 The section 3A offence is an either way offence, with a maximum penalty on indictment of two years imprisonment. That is surprising given that

232 www.wsj.com/Arts/its-official-north-korea-is-behind-wannacry-1513642537.

this section is also capable of applying to tools used for the most serious offending under the Act, pursuant to section 3ZA, for which the maximum penalty is life imprisonment. It may be therefore that in future this maximum penalty is revised upwards.

TERRITORIAL SCOPE

Sections 4 and 5

3.144 The Act originally provided for a degree of extra-territorial jurisdiction. As enacted, the Act ensured that a person could be prosecuted for an offence under section 1 or section 3 that had been committed abroad, provided that there was a 'significant link' to the UK.

3.145 The extra-territorial jurisdiction of the Act was widened by the Serious Crime Act 2015 (SCA 2015). It not only amended section 4 to extend extra territorial jurisdiction to section 3A and to the newly created section 3ZA offence, but also inserted the new sections 5(1A) and (1B), the effect of which was to increase the scope of the Act considerably; those sections allow the prosecution of UK nationals for Computer Misuse Act offences regardless of whether or not the conduct has any other link to the UK, as long as the conduct also amounts to an offence in the country in which it took place.

3.146 Section 5 of the Act was also amended by the SCA 2015 to define what constitutes a 'significant link' to the UK, in order to ensure that the ability to prosecute non-UK nationals under the Act was enhanced. In essence, as originally enacted, a significant link was established if the suspect was in the UK at the time of the alleged offence. The SCA 2015 extended this to catch scenarios where the *individual* was not present in the UK at the time of the offence, but that the *computer or data accessed* was.

3.147 In the case of section 3ZA an additional possibility exists to extend the extra-territorial jurisdiction of the Act. A section 3ZA offence is still committed If the suspect 'caused or created a risk of material damage' to the UK, even if neither he nor the computer or data accessed where not within the UK at the time of the access.

Sentences

3.148 As yet, there are no sentencing guidelines issued by the Sentencing Council in respect of the Computer Misuse Act. As a result, various precedents may be of assistance to practitioners in their submissions to a sentencing court.

3.149 In *R v Mangham* [2012] EWCA Crim 973, the Court of Appeal quashed a sentence of eight months' imprisonment imposed at first instance and substituted four months' imprisonment concurrent for a 26 year old defendant who had

entered guilty pleas to three counts securing unauthorised access to computer material with intent, contrary section 1; and a further count of unauthorised modification of computer material, contrary to section 3.

3.150 The brief facts of the case were that the defendant, engaged in a sophisticated and persistent course of conduct to hack into Facebook servers and succeeded in downloading part of the Facebook source code onto his own devices. It was accepted that he had not acted for financial gain, albeit that his actions had cost Facebook some $200,000 in investigating and repairing the breach.

3.151 At paragraph 19 of the Judgment, the Court provided useful guidance as to the aggravating and mitigating factors that might be present in a Computer Misuse Act prosecution:

> 'From these authorities we would identify a number of aggravating factors which will bear on sentence in this type of case: firstly, whether the offence is planned and persistent and then the nature of the damage caused to the system itself and to the wider public interest such as national security, individual privacy, public confidence and commercial confidentiality. The other side of the coin to the damage caused will be the cost of remediation, although we do not regard that as a determining factor. Next, motive and benefit are also relevant. Revenge, which was a feature in Lindesay and Baker, is a serious aggravating factor. Further, the courts are likely to take a very dim view where a hacker attempts to reap financial benefit by the sale of information which has been accessed. Whether or not the information is passed onto others is another factor to be taken into account. The value of the intellectual property involved may also be relevant to sentencing. Among the mitigating factors the psychological profile of an offender will deserve close attention.'

3.152 As well as identifying a number of other factors, the Court gave particular regard to the psychology of the defendants in these matters; Mangham himself had been diagnosed with an Autism Spectrum Disorder and was described by the Court as 'relatively young in years but possibly emotionally younger, and that he had a psychological and a personal make up which had led to the behaviour' (Paragraph 11). The need to identify the presence of any relevant mental health condition became a key element to the defence preparation of such matters.

3.153 *Mangham* was reconsidered by the Court of Appeal the following year, in *R v Martyn* [2013] EWCA Crim 1420. In that case, the Court took the view that Mr Martyn's appeal against a first instance of two years' imprisonment could not succeed.

3.154 Like Mangham, Martyn had entered guilty pleas to a number of offences; five offences of unauthorised modification of computer material contrary to section 3(1) of the Act (two years' imprisonment), one offence of securing unauthorised access to computer material with intent contrary to section 2(1)(a) (12 months' imprisonment), one offence of securing unauthorised access to computer material contrary to section 1 (six months' imprisonment)

and two offences of making, supplying or obtaining articles for use contrary to section 3(A) and (5) (four months' imprisonment). The sentences were to run concurrently, giving a total of two years' imprisonment.

3.155 Martyn's conduct had a number of aggravating factors that were not present in Mangahm. Those identified included the sophisticated planning behind the offending, the significant damage caused as a result of it, the potential consequences for the organisations targeted and the public interest in protecting them (Martyn's institutional targets were Universities' and Law Enforcement Agencies) and the invasion of privacy of Martyn's individual victims. Indeed the Court said that 'In our judgment, these offences fall into the highest level of culpability: they were carefully planned offences which did and were intended to cause harm both to the individuals and organisations targeted.' (Paragraph 36).

3.156 A further factor was the Defendant's lengthy criminal record of similar offences. The only significant mitigating factor taken into account was the fact that the offences had not been committed for personal gain.

3.157 Significantly, the Court took care to comment on the growing public interest in dealing harshly with cyber criminals:

> 39. The wider implications of such crimes for society cannot be ignored. Offences such as these, have the potential to cause great damage to the community at large and the public, as well as to the individuals more directly affected by them. Further, it is fortuitous and beyond the control of those who perpetrate them, whether they do so or not. This finds reflection in the maximum sentence which may be passed of ten years' imprisonment for an offence contrary to section3(1) of the Act and of five years' imprisonment for an offence contrary to section 2(1) of the Act. These offences are comparatively easy to commit by those with the relevant expertise, they are increasingly prevalent, and the public is entitled to be protected from them. In our view, it is appropriate for sentences for offences such as these to involve a real element of deterrence. Those who commit them must expect to be punished accordingly.

3.158 The Court also went on to specifically comment on the decision in Mangham, which had been heavily relied upon by the Defence in the Appeal, stating that:

> 43. Without seeking to undermine the mitigating features or the sentence in Mangham, in our judgment, it should not be considered a benchmark for such cases, which, in the ordinary course, are now likely to attract sentences that are very considerably longer: for offending of this scale, sentences will be measured in years rather than months. The prevalence of computer crime, its potential to cause enormous damage, both to the credibility of IT systems and the way in which our society now operates, and the apparent ease with which hackers, from the confines of their own homes, can damage important public institutions, not to say individuals, cannot be understated. The fact that organisations are compelled to spend substantial sums combating this type of crime, whether committed for gain or out of bravado, and the potential impact on individuals such

> as those affected in this case only underlines the need for a deterrent sentence.

3.159 However, despite the failure of the appeal and the obvious hardening of the Court's position in respect of the sentences to be imposed in such cases, the position was not entirely bleak for defendants; no issue was raised in respect of Mr Martyn's psychology and thus the Court expressed no view that would contradict the ruling in *Mangham* that psychological conditions such as Asperger's Syndrome deserved careful consideration in a sentencing exercise.

3.160 Finally, the recent case of *Mudd* [2017] EWCA Crim 1395 highlights that the Court of Appeal has continued in the direction of travel identified in *Martyn.*

3.161 In *Mudd* the defendant admitted operating the DDOS for hire service 'Titanium Stresser'. He entered guilty pleas to and was sentenced on a single count contrary to section 3(1) and (6) (24 months' detention in a young offender institution); an offence under section 3A of the Act (nine months' detention concurrent); and a single count of concealing criminal property, contrary to section 327(1) of the Proceeds of Crime Act 2002 (24 months' detention concurrent).

The total sentence imposed was, therefore, 24 months' detention in a young offender institution.

3.162 The scope of the offending was severe; Titanium Stresser had 112,298 registered users and in total, 1,738,828 attacks were carried out, directed against 666,532 individual IP addresses or domain names. In total, the appellant received some £248,000 from Titanium Stresser and other DDoS tools that he supplied.

3.163 Like Mangham, Mudd suffered from Autism and a number of reports were commissioned into his psychological condition and how this potentially affected his motives. The Court's opinion was plain: 'that condition cannot and does not absolve him from criminal responsibility. The judge said, very fairly, that where a diagnosis of autism or Asperger's is established, as the judge accepted it was in this case, that must be taken into account in determining the appropriate sentence. The question remained as to whether it should be determinative of what the sentence must be.'

3.164 Again, the Court in *Mudd* was concerned with 'the scale of criminality' and the 'very considerable public interest in and concern about criminality of this kind.'

> '…Offending of this kind, which was both facilitated by and carried out by this [appellant] has the potential to cause great and lasting damage, not only to those directly targeted but also to the public at large. It is now impossible to imagine a world without the internet. There is no part of life that is not touched by it in some way. These offences may be relatively easy to commit but they are increasingly prevalent and the public is entitled to be protected

from them. It follows that any sentence passed in a case of this level of seriousness must involve a real element of deterrence'. (paragraph 35)

3.165 The sentencing Court indicated that had the defendant been an adult of good character, convicted after a trial, the starting point would have been a custodial sentence of six years' imprisonment. However, in the light of the defendant's youth, psychological condition, and the delay between arrest and charge the Court was able to reduce that period substantially to 32 months' custody. That figure was reduced further by the Judge at first instance by 25% for Mr Mudd's early guilty plea, giving the total sentence of 24 months. The Judge chose not to exercise his discretion to suspend the sentence.

3.166 The Court of Appeal agreed with the sentencing Judge in all aspects, save the relatively minor point that the defendant should have been awarded full credit of 33% for his plea, not merely 25%. Thus his sentence following appeal was set at 21 months' custody in a Young Offenders Institute. A harsh sentence indeed in comparison with that handed to Mangham just five years earlier, and one that is anchored in the need to deter widespread online criminality and to protect the general public.

3.167 Unfortunately for defence practitioners, the line of the authorities is clear; the sentences imposed by Courts and upheld on Appeal have become steadily more severe as the true impact of this offending has become more readily understood.

The Future

3.168 It is difficult to see the extent to which the Computer Misuse Act will need to be updated to cope with future technological changes. However, it is clear that both the Act itself as well as the amendments made by the PJA 2006 and the SCA 2015 take into account the pace of change and have been deliberately drafted in an attempt to be as 'future proof' as possible. The wide scope of the definitions within the Act as well as its vast territorial scope are an intentional effort to ensure that the Act can, to the fullest extent possible, move with the times.

3.169 However, whilst the Act may be said to cover the potential offences that might be committed by an individual or a hacking group, one area where it is arguably deficient is in respect of the defences available to those under suspicion by the Authorities.

3.170 There are two areas where thought might be given to amending the Act in this way. Firstly, there is, at present no concept of 'cyber self defence' or of retaliating against an attacker in order to protect oneself or one's business from outside interference. At present, any individual gaining unauthorised access to an attacker's system would themselves potentially be at risk of Criminal liability under the Act.

3.171 The concept of 'hacking back' is not new and is extremely controversial, giving rise to legitimate concerns of cyber vigilante-ism. However the idea received a recent and significant boost in October 2017 when the 'Active Cyber Defense Certainty Bill' was introduced to the US Congress. The Bill is in the earliest stages but would, if passed into law, seek to act as a deterrent to cyber criminals by giving authorised individuals and companies the legal authority to leave their network to 1) establish attribution of an attack, 2) disrupt cyber-attacks without damaging others' computers, 3) retrieve and destroy stolen files, 4) monitor the behaviour of an attacker, and 5) utilise beaconing technology.[233] The Bill may well not pass into law, and even if it did, similar legislation might never be introduced in this country, but were it to do so, it would be interesting to see how it operated in practice.

3.172 Indeed it may be the case that hacking back, although risky unless adequately safeguarded, is now something that should be considered by the UK authorities. In an ideal scenario, there would be adequate resources available to public law enforcement bodies to enable them to deal with cyber threats. Although in comparison to other branches of law enforcement the UK's cybercrime investigators are well trained and resourced, the overall scale of the problem is such that they simply cannot investigate all breaches fully. In such circumstances it is arguable that private bodies should be permitted to defend themselves more aggressively.

3.173 That said, it may well be that the counter arguments are more persuasive; that many companies which are breached are breached because of the inadequacy of their defences, not through the sophistication of the attacker, and would therefore be unlikely to be able to hack back in any safe or meaningful way. One might also argue that in any event, in practical terms the risk of prosecution for hacking back, if done in a limited and proportionate fashion is vanishingly small and thus any amendment would deal with a risk to businesses that is largely theoretical.

3.174 In a similar vein, the Act could be amended to provide a degree of protection to Hacktivists or individuals who believe that their unauthorised access to a computer was justified in the public interest. It could be thought surprising that the Act does not contain such a defence already. As an example, the Criminal offence created by section 55 of the Data Protection Act 1998 of obtaining or disclosing personal data unlawfully (ie without the consent of the Data Controller) provides for two defences that are not available to those charged under section 1 of the Computer Misuse Act. Those defences are:

- At 55 (2)(c) that the individual acted in the reasonable belief that he would have had the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it, and
- At 55 (2)(d) that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.

233 https://tomgraves.house.gov/news/documentsingle.aspx?DocumentID=398840.

3.175 Thus, if amended in line with the section 55 of the DPA 1998, the CMA would protect an individual from criminal liability in circumstances where they had gained access to a computer system without authorisation but where they held a belief that access would have been authorised by an individual capable of providing authorisation, had they known of the circumstances of the access.

3.176 Equally, providing protection for those engaged in hacking in the public interest would assist in clarifying the status of so called 'ethical hackers'. Whilst this suggestion might call to mind controversial whistle-blowers such as Wikileaks and difficult considerations of whether those actions are genuinely in the public interest, the position is that such a provision might genuinely improve cyber security for businesses by enabling individuals to safely test for and report vulnerabilities in a system without fear of prosecution.

3.177 The absence of those potential defences does not, of course mean that the public interest is not a consideration; the full code test for Crown Prosecutors requires that when considering whether or not to prosecute, the reviewing lawyer should be satisfied firstly whether or not there is sufficient evidence to give a realistic prospect of conviction. If so, they must then consider whether it is in the public interest to bring a prosecution. Thus whilst the safeguard may not be as strong as it might be if it were enshrined in the Act, it does exist.

3.178 The Computer Misuse Act has been remarkably successful in dealing with the evolution of online crime in an era that has seen technology change our lives in a way that was scarcely imaginable when the Act was first drafted. The key to that success has been the wide scope of the offences and the broad definitions that are applicable, ensuring that it can cover a range of behaviours without requiring much amendment. As amended, the Act seems well set to extend its useful life well into the future. There are caveats for the unforeseeable of course; the pace of change is accelerating, not slowing down. Perhaps public policy will demand specific offences to prosecute those who interfere with a self-driving car, although such activity could also fall squarely within the existing offences. Equally, it may be that debate over future prosecutions under the Act bring the lack of a 'public interest' defence under scrutiny.

CHAPTER 4A

THE RISK PRACTITIONER'S JOURNEY: RISK ALIGNED ASSURANCE AND THE THREE LINES OF DEFENCE

Farid Abdelkader

SECTION 1: AN INTRODUCTION TO RISK ALIGNED ASSURANCE AND MY JOURNEY ACROSS THE THREE LINES OF DEFENCE

4.01 As a risk practitioner, I have always been passionate about identifying, assessing, and mitigating risks that organisations face. My extensive experience of over 18 years in a top 20 Risk Management Consulting organisation and years as a Global Head of Technology Audit for a Top 4 Mutual Insurance Company have allowed me to work across all three lines of defence in various industries, with a particular focus on insurance and banking.

4.02 My journey began in the first line as a help desk and systems engineer, which provided me with invaluable hands-on experience. As I progressed, I moved to the second line as a Risk Practitioner and Virtual CISO (V-CISO), where I honed my skills in risk assessment and mitigation. Eventually, I reached the pinnacle of my career at the consulting organisation, becoming the Managing Director of Technology Risk and Global Head of the firm's Cybersecurity Audit Pillar. Now, I serve as the Global Head of Technology Audit (third line of defence) for a global Fortune 75 Insurance Organization and President of the ISACA Metropolitan New York Metropolitan Chapter.

4.03 Over the years, I have witnessed the evolution of risk management strategies and frameworks that help organisations better prepare for and respond to risks. One such framework is Risk Aligned Assurance, which is grounded in the principles of the Three Lines of Defence model. Initially introduced during the dot-com bubble burst (~2000), the Three Lines of Defence model was introduced by the Institute of Internal Auditors' (IIA) standards (2013) and has become a cornerstone of risk management practices. Its impact and relevance have also led to its widespread adoption into banking by the Office of the Comptroller of the Currency (OCC) as part of the Code of Federal Regulations (CFR) 12 Part 30. This widespread adoption impacted not just in banking, but various industries.

4.04 In this chapter, I will take you through my personal journey of Risk Aligned Assurance and its development through the Three Lines of Defence.

I will also delve into the importance of this approach across industries and explore real-life case studies that demonstrate the benefits of aligned assurance, including independence in risk coverage, comprehensive risk coverage, cost savings, and more. As we embark on this journey together, you will gain valuable insights into the world of risk management from my firsthand experiences and learn how Risk Aligned Assurance has become an essential part of modern risk management practices.

SECTION 2: THE BEGINNING – OCC'S CFR 12 PART 30, GLOBAL REGULATIONS, AND THE THREE LINES OF DEFENCE

4.05 The roots of formalised Risk Aligned Assurance can be traced back to the Three Lines of Defence model, introduced by the OCC in CFR 12 Part 30. The OCC, responsible for regulating and supervising national banks and federal savings associations in the United States, recognised the importance of a robust risk management framework, particularly in the aftermath of financial crises and increasing regulatory scrutiny.

4.06 CFR 12 Part 30, or the 'Safety and Soundness Standards' regulation, outlines guidelines and expectations for national banks and federal savings associations concerning risk management practices. It aims to ensure the safety and soundness of financial institutions and promote a more resilient financial system. The Three Lines of Defence model is central to these guidelines and has been incorporated into other global regulations and best practices, such as the Bermudian Code of Conduct for Corporate Governance (CCC), New York Department of Financial Services (NY DFS) 23 NYCRR 500, General Data Protection Regulation (GDPR), and other relevant international regulations.

4.07 The Three Lines of Defence model consists of:

1. **First Line of Defence:** Business operations and management, responsible for identifying, assessing, and managing risks within their day-to-day activities, implementing risk control measures, and ensuring compliance with policies and regulations.
2. **Second Line of Defence:** Risk management and compliance functions, tasked with providing oversight and support to the first line, developing risk management frameworks, policies, and procedures, and monitoring the effectiveness of risk controls.
3. **Third Line of Defence:** Internal audit functions, providing independent assurance on the effectiveness of risk management, internal controls, and governance processes while reporting directly to the board or audit committee to ensure objectivity and independence.

4.08 The model's simplicity and effectiveness in promoting clear roles and responsibilities for risk management made it appealing to organisations beyond the banking sector, with industries such as healthcare, manufacturing, and

technology adopting it as a foundation for their risk management practices. Its widespread adoption also caught the attention of the IIA, which incorporated the model into its standards, further cementing its importance in the risk management landscape.

4.09 Global regulations and best practices, such as the Bermudian CCC, NY DFS 23 NYCRR 500, GDPR, and others, have contributed to the widespread adoption of the Three Lines of Defence model. These regulations emphasise a structured approach to managing risk across various lines of defence, including technology, privacy, and cybersecurity risks.

4.10 As organisations navigate the complexities of an increasingly interconnected and regulated world, the Three Lines of Defence model offers a structured approach to managing risk. This alignment of assurance across the three lines of defence enables organisations to be more resilient and better prepared for potential threats.

4.11 Risk Aligned Assurance has become a critical component of risk management for organisations worldwide, enabling them to better identify, assess, and mitigate risks while ensuring compliance with various global regulations. By embracing this approach and the principles of the Three Lines of Defence model, organisations can create a more robust risk management culture that supports their long-term success and resilience in the face of evolving challenges.

SECTION 3: RISK ALIGNED ASSURANCE – THE EVOLUTION OF THE THREE LINES OF DEFENCE AND THE EMERGENCE OF ALIGNED ASSURANCE

4.12 As the Three Lines of Defence model gained traction, organisations began to recognise the need for a more integrated approach to risk management. This realisation led to the development of Risk Aligned Assurance – an approach that builds upon the Three Lines of Defence model by emphasising the alignment of risk management activities across the organisation. This evolution was further reinforced by the Institute of Internal Auditors' (IIA) insights on the model, highlighting the importance of clarity, collaboration, and continuous improvement in risk management.

4.13 Risk Aligned Assurance enhances the Three Lines of Defence by:

- **Ensuring clear communication and collaboration between the three lines:** This fosters a shared understanding of risk and promotes a consistent approach to risk management across the organisation. For instance, the first line shares information about identified risks and control measures with the second line, which in turn provides oversight and guidance on risk mitigation strategies. The third line then independently evaluates the effectiveness of the risk management framework and provides feedback for improvement.

- **Encouraging the integration of risk management activities into the organisation's core processes and decision-making:** By embedding risk management into day-to-day operations, organisations can proactively address risks and improve overall performance. For example, integrating cybersecurity controls into application development processes can help prevent potential data breaches and protect sensitive information.
- **Focusing on the continuous improvement of risk management practices:** Risk Aligned Assurance encourages organisations to regularly assess and enhance their risk management processes, frameworks, and controls, ensuring they remain effective in a constantly changing risk environment. This might involve implementing new technologies, updating policies and procedures to address emerging risks, or refining risk assessment methodologies based on lessons learned.
- **Promoting a risk-aware culture:** A key aspect of Risk Aligned Assurance is cultivating a culture where all employees understand their role in managing risks and are empowered to take appropriate actions to mitigate them. For instance, organisations can invest in ongoing risk awareness training and communication initiatives and recognise and reward employees who proactively identify and address risks.

4.14 The evolution of the Three Lines of Defence model into Risk Aligned Assurance has allowed organisations to reap significant benefits from its structured approach. The alignment of risk management activities across the organisation enables more efficient and effective risk mitigation, leading to cost savings, better risk coverage, and enhanced independence in risk assessments.

4.15 Moreover, the incorporation of global regulations, such as the Bermudian Corporate Governance Code (CCC), New York Department of Financial Services (NY DFS) 23 NYCRR 500, and the General Data Protection Regulation (GDPR), into risk management frameworks has further emphasised the importance of a strong, aligned risk management structure. By adhering to the principles of Risk Aligned Assurance, organisations can better navigate the complexities of these regulations and ensure compliance while addressing various technology, privacy, and cybersecurity risks.

SECTION 4: RISK ALIGNED ASSURANCE AND ITS LEVERAGE ACROSS INDUSTRIES

4.16 While the Three Lines of Defence model and Risk Aligned Assurance originated in the banking sector, their principles have proven valuable across various industries. The need for effective risk management is universal, as all organisations face a range of risks that can impact their ability to achieve their objectives.

4.17 In the healthcare industry, for example, the alignment of risk management activities can help organisations better anticipate and address risks related to

patient safety, data security, and regulatory compliance. By ensuring that all three lines of defence work together to manage these risks, healthcare providers can improve patient outcomes and reduce the likelihood of adverse events.

4.18 Similarly, manufacturing companies can benefit from Risk Aligned Assurance by identifying and managing risks related to product quality, supply chain disruptions, and workplace safety. By adopting a unified approach to risk management, manufacturers can improve the efficiency of their operations and minimise the impact of disruptions.

4.19 Technology companies, too, can leverage Risk Aligned Assurance to address risks related to cybersecurity, data privacy, and rapid technological changes. By aligning their risk management efforts, technology companies can better protect their assets and maintain their competitive edge in an increasingly digital world.

4.20 Moreover, even in industries that are not as heavily regulated, Risk Aligned Assurance has proven to be valuable. For instance, the Payment Card Industry Data Security Standard (PCI DSS) requires organisations that handle cardholder data to implement a comprehensive risk management framework. By applying the principles of Risk Aligned Assurance, organisations can ensure compliance with PCI DSS requirements while effectively managing risks associated with cardholder data security.

SECTION 5: CASE STUDIES – THE BENEFITS OF ALIGNED ASSURANCE

4.21 To fully understand the value of Risk Aligned Assurance, let's examine some case studies that demonstrate its benefits, including independence in risk coverage, comprehensive risk coverage, cost savings, and more.

Case Study 1: Independence in Risk Coverage – A Global Bank

A large global bank recognised the need to strengthen its risk management practices in the wake of increased regulatory scrutiny, such as Basel III standards and the Dodd-Frank Wall Street Reform and Consumer Protection Act. The bank implemented Risk Aligned Assurance, ensuring clear communication and collaboration between the three lines of defence. This alignment allowed the third line (internal audit) to maintain its independence while providing assurance on the effectiveness of risk management activities carried out by the first and second lines.

As a result, the bank was able to identify gaps in its risk management processes and address them proactively, leading to a more robust risk management framework and increased confidence from regulators and stakeholders.

Case Study 2: Comprehensive Risk Coverage – A Healthcare Provider

A large healthcare provider faced numerous risks related to patient safety, data security, and regulatory compliance, such as the Health Insurance Portability and Accountability Act (HIPAA) and the European Union's General Data