

# CONTENTS

## PART 1 — AN AERIAL SURVEY OF INFORMATION SECURITY

|                  |                                        |           |
|------------------|----------------------------------------|-----------|
| <b>Chapter 1</b> | <b>What is information security?</b>   | <b>3</b>  |
|                  | A New Kind of Mayhem                   | 3         |
|                  | Mapping the Boundaries and Terrain     | 7         |
|                  | Confidentiality                        | 7         |
|                  | Integrity                              | 8         |
|                  | Availability                           | 9         |
|                  | “Acceptable Use”                       | 10        |
|                  | “Foundation Concepts”                  | 11        |
|                  | Security, Cost and Usability           | 11        |
|                  | Layers                                 | 15        |
|                  | People, Process and Technology         | 17        |
|                  | How Much Security is “Enough”?         | 18        |
| <b>Chapter 2</b> | <b>External threats</b>                | <b>23</b> |
|                  | Criminals With Keyboards               | 23        |
|                  | The Dark Number                        | 25        |
|                  | A Market Driven Thing                  | 27        |
|                  | Popular Misconceptions                 | 28        |
|                  | How does it happen?                    | 29        |
|                  | Exploiting Vulnerable “Holes”          | 29        |
|                  | The Weak Firewall                      | 31        |
|                  | Administrator Passwords                | 32        |
|                  | User Log On Credentials                | 33        |
|                  | Carelessness                           | 34        |
|                  | Keystroke Logging Software and Spyware | 34        |
|                  | “Phishing” and “Spear Phishing”        | 35        |
|                  | Insecure Web Applications              | 35        |
|                  | Insecure Wireless Networks             | 36        |
|                  | Social Engineering                     | 37        |
| <b>Chapter 3</b> | <b>Inside jobs and data leakage</b>    | <b>43</b> |
|                  | Introduction                           | 43        |
|                  | Inside Jobs                            | 43        |
|                  | The “Bad Apple”                        | 43        |
|                  | “Self Helpers”                         | 46        |
|                  | What Can Be Done?                      | 47        |
|                  | Disabling USB Ports                    | 47        |
|                  | Access Controls                        | 47        |
|                  | Access Logging                         | 49        |
|                  | Email Filtering                        | 49        |
|                  | Terminating Employee Access            | 49        |
|                  | The Balance of Convenience             | 50        |
|                  | Accidental Data Leakage                | 51        |
|                  | Lost and Stolen Laptops                | 51        |

|                                              |                                                                                                                    |            |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------|------------|
|                                              | Other Mobile Storage Devices .....                                                                                 | 54         |
|                                              | Email Accidents .....                                                                                              | 56         |
|                                              | Other Types of Data Leakage .....                                                                                  | 58         |
| <b>PART 2 — “DUTIES? WHAT DUTIES?”</b>       |                                                                                                                    |            |
| <b>Chapter 4 The battlegrounds.....</b>      |                                                                                                                    | <b>63</b>  |
|                                              | Introduction .....                                                                                                 | 63         |
|                                              | Theft or Leakage of Credit/Debit Card Information: The TJX Case ..                                                 | 64         |
|                                              | TJX — The Facts.....                                                                                               | 64         |
|                                              | The Background to Credit and Debit Card Transactions.....                                                          | 65         |
|                                              | TJX — The Legal Actions.....                                                                                       | 67         |
|                                              | TJX — The Settlement.....                                                                                          | 68         |
|                                              | Theft or Leakage of Personal Information and Invasion of Privacy.....                                              | 69         |
|                                              | The ABC Case.....                                                                                                  | 69         |
|                                              | The Potential Implications.....                                                                                    | 70         |
|                                              | Theft or Leakage of Commercially Confidential Information .....                                                    | 71         |
|                                              | The Goodyear Episode .....                                                                                         | 71         |
|                                              | The ClearOne Episode.....                                                                                          | 72         |
|                                              | Third Party Information: The Neggear Episode.....                                                                  | 73         |
|                                              | Physical Loss or Damage Flowing From an Interruption of a<br>Computerised Industrial/Operational Environment ..... | 74         |
|                                              | The Seattle Hospital Episode .....                                                                                 | 76         |
|                                              | The PER Oil Pipeline Episode.....                                                                                  | 78         |
| <b>Chapter 5 The tort of negligence.....</b> |                                                                                                                    | <b>79</b>  |
|                                              | Overview of Duty of Care in Negligence .....                                                                       | 79         |
|                                              | Theft or Leakage of Credit/Debit Card Information: The TJX Case ..                                                 | 81         |
|                                              | The Pure Economic Loss Doctrine in Australia.....                                                                  | 83         |
|                                              | A Synthesis? .....                                                                                                 | 87         |
|                                              | Conclusions.....                                                                                                   | 89         |
|                                              | Negligent Misrepresentation.....                                                                                   | 89         |
|                                              | Theft or Leakage of Personal Information and Invasion of Privacy.....                                              | 91         |
|                                              | Broader Application .....                                                                                          | 92         |
|                                              | Theft or Leakage of Commercially Confidential Information .....                                                    | 93         |
|                                              | Physical Loss or Damage Flowing From an Interruption of a<br>Computerised Industrial/Operational Environment ..... | 95         |
|                                              | Conclusions.....                                                                                                   | 99         |
| <b>Chapter 6 Privacy legislation.....</b>    |                                                                                                                    | <b>101</b> |
|                                              | Introduction .....                                                                                                 | 101        |
|                                              | The Concept of Privacy .....                                                                                       | 102        |
|                                              | The Role of the Privacy Commission .....                                                                           | 103        |
|                                              | Privacy Legislation in Australia .....                                                                             | 104        |
|                                              | The Privacy Principles .....                                                                                       | 105        |
|                                              | Compensation for Breach of the Privacy Act.....                                                                    | 106        |
|                                              | Tort of Breach of Statutory Duty?.....                                                                             | 108        |
|                                              | A New Statutory Cause of Action for a Serious Invasion of Privacy? .                                               | 109        |
|                                              | Scope .....                                                                                                        | 110        |

|                   |                                                                                      |            |
|-------------------|--------------------------------------------------------------------------------------|------------|
|                   | Applying the Tests.....                                                              | 112        |
|                   | Conclusions.....                                                                     | 114        |
| <b>Chapter 7</b>  | <b>Privacy at common law.....</b>                                                    | <b>115</b> |
|                   | Introduction .....                                                                   | 115        |
|                   | Breach of Confidence .....                                                           | 116        |
|                   | Expanding the Ambit of Breach of Confidence .....                                    | 116        |
|                   | Is the Information “Private” — and What About Freedom of<br>Expression? .....        | 119        |
|                   | Extension to Cases of Data Leakage?.....                                             | 120        |
|                   | Tort of Invasion of Privacy.....                                                     | 125        |
|                   | Application to Information Security.....                                             | 127        |
|                   | Conclusions.....                                                                     | 129        |
| <b>Chapter 8</b>  | <b>Contract.....</b>                                                                 | <b>131</b> |
|                   | Introduction .....                                                                   | 131        |
|                   | Non Disclosure and Confidentiality Agreements (and Confidentiality<br>Clauses) ..... | 133        |
|                   | Non Disclosure Agreements.....                                                       | 133        |
|                   | Other Similar Documents.....                                                         | 134        |
|                   | Specific Provisions.....                                                             | 136        |
|                   | Implications.....                                                                    | 138        |
|                   | Implied Contracts.....                                                               | 140        |
|                   | Extended Enterprises .....                                                           | 141        |
|                   | Compliance Driven Contracts.....                                                     | 144        |
|                   | Contractual Indemnity Provisions .....                                               | 145        |
|                   | Conclusions.....                                                                     | 148        |
| <b>Chapter 9</b>  | <b>Trade Practices Act &amp; related legislation.....</b>                            | <b>151</b> |
|                   | Overview of the Trade Practices Act.....                                             | 151        |
|                   | Main Elements .....                                                                  | 153        |
|                   | Broad Applicability.....                                                             | 155        |
|                   | Applicability to Information Security.....                                           | 155        |
|                   | Theft or Leakage of Credit/Debit Card Information .....                              | 156        |
|                   | Theft or Leakage of Personal Information .....                                       | 157        |
|                   | Theft or Leakage of Commercially Confidential Information ..                         | 158        |
|                   | Conclusions.....                                                                     | 163        |
| <b>Chapter 10</b> | <b>Other liability scenarios.....</b>                                                | <b>165</b> |
|                   | Introduction .....                                                                   | 165        |
|                   | Personal Liabilities of Directors and Officers.....                                  | 165        |
|                   | Overview of Directors’ Duties.....                                                   | 165        |
|                   | To Whom Are The Duties Owed?.....                                                    | 168        |
|                   | Applicability to Information Security.....                                           | 170        |
|                   | Criminal Liability .....                                                             | 175        |
|                   | Vicarious Liability .....                                                            | 177        |
|                   | Overview .....                                                                       | 177        |
|                   | Application To Information Security.....                                             | 179        |
|                   | Conclusions.....                                                                     | 182        |

**PART 3 — DUTIES, STANDARDS, AND PROTECTIVE MEASURES**

|                                                                                  |            |
|----------------------------------------------------------------------------------|------------|
| <b>Introduction to Part 3 .....</b>                                              | <b>187</b> |
| The Causal Chain.....                                                            | 187        |
| The Required Standard of Care .....                                              | 187        |
| <b>Chapter 11 Reasonable care.....</b>                                           | <b>191</b> |
| “Reasonable Care” — The Search for a Benchmark: Standards .....                  | 191        |
| ISO/IEC 27001.....                                                               | 192        |
| ISO/IEC 17799.....                                                               | 194        |
| Sarbanes-Oxley & COBIT .....                                                     | 196        |
| PCI DSS .....                                                                    | 199        |
| “Reasonable Care” — The Search for a Benchmark: Investigative<br>Decisions ..... | 202        |
| Reasonable Care: Context and Conduct .....                                       | 204        |
| Risk Assessments.....                                                            | 204        |
| Documented Policies and Procedures.....                                          | 206        |
| Conclusions.....                                                                 | 213        |
| <b>Chapter 12 Risk management .....</b>                                          | <b>215</b> |
| Introduction .....                                                               | 215        |
| Practical Implementation of a Risk Management Regime .....                       | 216        |
| First Step: Understanding the Business Processes .....                           | 217        |
| Second Step: Understanding the Assets in Play & their Attributes ....            | 218        |
| Physical Assets .....                                                            | 219        |
| Information Assets .....                                                         | 219        |
| Software Assets and Services.....                                                | 219        |
| Network Architecture .....                                                       | 220        |
| Third Step: Relating the Assets to the Business Processes .....                  | 223        |
| Fourth Step: Identifying Risks .....                                             | 224        |
| Fifth Step: Assessing the Risk.....                                              | 229        |
| Sixth Step: Acceptance or Treatment.....                                         | 230        |
| Seventh Step: Assessing the Impact of Treatments.....                            | 231        |
| Final Step: The Risk Register .....                                              | 232        |
| Conclusions.....                                                                 | 235        |
| <b>Chapter 13 Controls: policies and procedures.....</b>                         | <b>237</b> |
| Introduction .....                                                               | 237        |
| Structure.....                                                                   | 237        |
| The “Boilerplate Policies” Myth.....                                             | 242        |
| The “Sections” .....                                                             | 244        |
| Organisation of Information Security .....                                       | 248        |
| Roles and Responsibilities .....                                                 | 249        |
| External Security Reviews .....                                                  | 249        |
| Asset Management.....                                                            | 251        |
| Information Classification.....                                                  | 252        |
| Encryption.....                                                                  | 256        |
| Human Resources Security .....                                                   | 258        |
| Physical and Environmental Security.....                                         | 259        |
| Communications and Operations Management .....                                   | 260        |
| Change Management.....                                                           | 261        |
| Protections Against Malware.....                                                 | 263        |

|                                                                  |            |
|------------------------------------------------------------------|------------|
| Access Controls .....                                            | 268        |
| Privileged Access .....                                          | 269        |
| User Responsibilities For Passwords .....                        | 269        |
| Information Systems Acquisition, Development & Maintenance.....  | 271        |
| Patch Management .....                                           | 271        |
| Information Security Incident Management .....                   | 276        |
| Business Continuity Management .....                             | 278        |
| DRP .....                                                        | 280        |
| Business Continuity .....                                        | 284        |
| Compliance .....                                                 | 286        |
| External Compliance .....                                        | 286        |
| Internal Compliance .....                                        | 287        |
| User Version(s) of Policy Sets .....                             | 288        |
| Conclusions .....                                                | 289        |
| <b>Chapter 14 Contractual obligations .....</b>                  | <b>291</b> |
| Introduction .....                                               | 291        |
| Defensive Strategies .....                                       | 291        |
| Acceptable Use Agreements .....                                  | 293        |
| A Question of Style.....                                         | 294        |
| The Preface to the AUA .....                                     | 295        |
| Linkage with Information Security Policy Set.....                | 296        |
| Monitoring and Surveillance.....                                 | 296        |
| Illegal or Improper Use .....                                    | 298        |
| Disciplinary Issues and Compensation.....                        | 299        |
| Contractual Warranties, Indemnities and Pre-Contract             |            |
| “Due Diligence” .....                                            | 300        |
| Joint Venture Agreements .....                                   | 300        |
| Acquisitions .....                                               | 302        |
| Outsourcing Agreements .....                                     | 303        |
| Conclusions.....                                                 | 306        |
| <b>Chapter 15 Reflections, predictions, and next steps .....</b> | <b>309</b> |
| When is a Risk Not a Risk?.....                                  | 309        |
| Getting the Board Onside.....                                    | 311        |
| Evolution in Legal Practice .....                                | 312        |
| The Tidal Wave and the Sea Defences.....                         | 314        |
| The False Prophets.....                                          | 315        |
| Where to From Here? .....                                        | 316        |
| Appendix 1 ISO/IEC 17799 Sections — Full List .....              | 319        |
| Appendix 2 Sources of Further Information.....                   | 327        |
| Appendix 3 Glossary of Legal Terms and Concepts.....             | 329        |
| Appendix 4 Glossary of Information Security and IT Terms and     |            |
| Concepts .....                                                   | 336        |
| Case Table .....                                                 | 347        |
| Legislation Table.....                                           | 351        |
| Index .....                                                      | 353        |