



Contents

| | |
|---|------------|
| Foreword | xv |
| Introduction | xix |
| Chapter 1 End of Life for Data | 1 |
| 1.1 Growth of Data | 3 |
| 1.2 Managing Data | 4 |
| 1.2.1 Discovery | 4 |
| 1.2.2 Classification | 5 |
| 1.2.3 Risk | 6 |
| 1.3 Data Loss | 6 |
| 1.3.1 Accidental | 7 |
| 1.3.2 Theft | 7 |
| 1.3.3 Dumpster Diving | 9 |
| 1.4 Encryption | 9 |
| 1.5 Data Discovery | 9 |
| 1.6 Regulations | 10 |
| 1.7 Security | 10 |
| 1.8 Legal Discovery | 11 |
| 1.9 Data Sanitization | 12 |
| 1.10 Ecological and Economic Considerations | 13 |
| 1.10.1 Ecological | 13 |
| 1.10.2 Economic | 13 |
| 1.11 Summary: Proactive Risk Reduction and Reactive End of Life | 14 |
| Chapter 2 Where Are We, and How Did We Get Here? | 15 |
| 2.1 Digital Data Storage | 16 |
| 2.2 Erasing Magnetic Media | 17 |
| 2.3 History of Data Erasure | 17 |

| | | |
|------------------|---|-----------|
| 2.3.1 | The Beginnings of Commercial Data Erasure | 19 |
| 2.3.2 | Darik's Boot and Nuke (DBAN) | 19 |
| 2.4 | Summary | 21 |
| Chapter 3 | Data Sanitization Technology | 23 |
| 3.1 | Shredding | 24 |
| 3.2 | Degaussing | 24 |
| 3.3 | Overwriting | 25 |
| 3.4 | Crypto-Erase | 27 |
| 3.5 | Erasing Solid-State Drives | 28 |
| 3.6 | Bad Blocks | 29 |
| 3.7 | Data Forensics | 29 |
| 3.8 | Summary | 31 |
| Chapter 4 | Information Lifecycle Management | 33 |
| 4.1 | Information Lifecycle Management vs. Data Lifecycle Management | 33 |
| 4.2 | Information Lifecycle Management | 34 |
| 4.2.1 | Lifecycle Stages | 34 |
| 4.3 | Data Security Lifecycle | 35 |
| 4.3.1 | Stages for Data Security Lifecycle | 36 |
| 4.4 | Data Hygiene | 36 |
| 4.5 | Data Sanitization | 37 |
| 4.5.1 | Physical Destruction | 37 |
| 4.5.2 | Cryptographic Erasure | 37 |
| 4.5.3 | Data Erasure | 38 |
| 4.6 | Summary | 39 |
| Chapter 5 | Regulatory Requirements | 41 |
| 5.1 | Frameworks | 42 |
| 5.1.1 | NIST Cybersecurity Framework Applied to Data | 42 |
| 5.2 | Regulations | 43 |
| 5.2.1 | GDPR | 44 |
| 5.2.1.1 | The Right to Erasure | 45 |
| 5.2.1.2 | Data Retention | 51 |
| 5.2.2 | HIPAA Security Rule Subpart C | 53 |
| 5.2.3 | PCI DSS V3.2 Payment Card Industry Requirements | 56 |
| 5.2.4 | Sarbanes–Oxley | 58 |
| 5.2.5 | Saudi Arabian Monetary Authority Payment Services Regulations | 59 |
| 5.2.6 | New York State Cybersecurity Requirements of Financial Services Companies 23 NYCRR 500 | 59 |
| 5.2.7 | Philippines Data Privacy Act 2012 | 60 |
| 5.2.8 | Singapore Personal Data Protection Act 2012 | 61 |
| 5.2.9 | Gramm–Leach–Bliley Act | 61 |

| | | |
|------------------|---|-----------|
| 5.3 | Standards | 62 |
| 5.3.1 | ISO 27000 and Family | 62 |
| 5.3.2 | NIST SP 800-88 | 63 |
| 5.4 | Summary | 65 |
| Chapter 6 | New Standards | 67 |
| 6.1 | IEEE P2883 Draft Standard for Sanitizing Storage | 68 |
| 6.1.1 | Data Sanitization | 68 |
| 6.1.2 | Storage Sanitization | 68 |
| 6.1.3 | Media Sanitization | 68 |
| 6.1.4 | Clear | 69 |
| 6.1.5 | Purge | 69 |
| 6.1.6 | Destruct | 69 |
| 6.2 | Updated ISO/IEC CD 27040 Information Technology Security Techniques—Storage Security | 70 |
| 6.3 | Summary | 71 |
| Chapter 7 | Asset Lifecycle Management | 73 |
| 7.1 | Data Sanitization Program | 73 |
| 7.2 | Laptops and Desktops | 74 |
| 7.3 | Servers and Network Gear | 76 |
| 7.3.1 | Edge Computing | 78 |
| 7.4 | Mobile Devices | 79 |
| 7.4.1 | Crypto-Erase | 80 |
| 7.4.2 | Mobile Phone Processing | 80 |
| 7.4.3 | Enterprise Data Erasure for Mobile Devices | 81 |
| 7.4.3.1 | Bring Your Own Device | 81 |
| 7.4.3.2 | Corporate-Issued Devices | 81 |
| 7.5 | Internet of Things: Unconventional Computing Devices | 82 |
| 7.5.1 | Printers and Scanners | 82 |
| 7.5.2 | Landline Phones | 82 |
| 7.5.3 | Industrial Control Systems | 82 |
| 7.5.4 | HVAC Controls | 83 |
| 7.5.5 | Medical Devices | 83 |
| 7.6 | Automobiles | 83 |
| 7.6.1 | Off-Lease Vehicles | 84 |
| 7.6.2 | Used Vehicle Market | 85 |
| 7.6.3 | Sanitization of Automobiles | 85 |
| 7.7 | Summary | 86 |
| Chapter 8 | Asset Disposition | 87 |
| 8.1 | Contracting and Managing Your ITAD | 88 |
| 8.2 | ITAD Operations | 89 |
| 8.3 | Sustainability and Green Tech | 91 |
| 8.4 | Contribution from R2 | 91 |
| 8.4.1 | Tracking Throughput | 91 |
| 8.4.2 | Data Security | 92 |

| | | |
|-------------------|---|------------|
| 8.5 | e-Stewards Standard for Responsible Recycling and Reuse of Electronic Equipment | 92 |
| 8.6 | i-SIGMA | 93 |
| 8.7 | FACTA | 93 |
| 8.8 | Summary | 95 |
| Chapter 9 | Stories from the Field | 97 |
| 9.1 | 3stepIT | 98 |
| 9.2 | TES – IT Lifecycle Solutions | 101 |
| 9.2.1 | Scale of Operations | 103 |
| 9.2.2 | Compliance | 104 |
| 9.2.3 | Conclusion | 104 |
| 9.3 | Ingram Micro | 104 |
| 9.4 | Summary | 106 |
| Chapter 10 | Data Center Operations | 109 |
| 10.1 | Return Material Allowances | 110 |
| 10.2 | NAS | 110 |
| 10.3 | Logical Drives | 110 |
| 10.4 | Rack-Mounted Hard Drives | 111 |
| 10.5 | Summary | 112 |
| Chapter 11 | Sanitizing Files | 113 |
| 11.1 | Avoid Confusion with CDR | 113 |
| 11.2 | Erasing Files | 114 |
| 11.3 | When to Sanitize Files | 115 |
| 11.4 | Sanitizing Files | 116 |
| 11.5 | Summary | 116 |
| Chapter 12 | Cloud Data Sanitization | 117 |
| 12.1 | User Responsibility vs. Cloud Provider Responsibility | 117 |
| 12.2 | Attacks Against Cloud Data | 119 |
| 12.3 | Cloud Encryption | 119 |
| 12.4 | Data Sanitization for the Cloud | 120 |
| 12.5 | Summary | 121 |
| Chapter 13 | Data Sanitization and Information Lifecycle Management | 123 |
| 13.1 | The Data Sanitization Team | 124 |
| 13.2 | Identifying Data | 124 |
| 13.3 | Data Sanitization Policy | 124 |
| 13.3.1 | Deploy Technology | 125 |
| 13.3.2 | Working with DevOps | 125 |
| 13.3.3 | Working with Data Security | 125 |
| 13.3.4 | Working with the Legal Team | 125 |
| 13.3.5 | Changes | 126 |
| 13.4 | Summary | 126 |

| | | |
|-------------------|--|------------|
| Chapter 14 | How Not to Destroy Data | 127 |
| 14.1 | Drilling | 127 |
| 14.1.1 | Nail Gun | 128 |
| 14.1.2 | Gun | 128 |
| 14.2 | Acids and Other Solvents | 128 |
| 14.3 | Heating | 128 |
| 14.4 | Incineration | 129 |
| 14.5 | Street Rollers | 129 |
| 14.6 | Ice Shaving Machines | 129 |
| Chapter 15 | The Future of Data Sanitization | 131 |
| 15.1 | Advances in Solid-State Drives | 132 |
| 15.2 | Shingled Magnetic Recording | 133 |
| 15.3 | Thermally Assisted Magnetic Recording, Also Known as Heat-Assisted Magnetic Recording | 133 |
| 15.4 | Microwave-Assisted Magnetic Recording | 134 |
| 15.5 | DNA Data Storage | 135 |
| 15.6 | Holographic Storage | 135 |
| 15.7 | Quantum Storage | 136 |
| 15.8 | NVDIMM | 137 |
| 15.9 | Summary | 138 |
| Chapter 16 | Conclusion | 139 |
| Appendix | Enterprise Data Sanitization Policy | 143 |
| | Introduction | 143 |
| | Intended Audience | 143 |
| | Purpose of Policy | 144 |
| | General Data Hygiene and Data Retention | 144 |
| | Data Spillage | 144 |
| | Handling Files Classified as Confidential | 144 |
| | Data Migration | 144 |
| | End of Life for Classified Virtual Machines | 145 |
| | On Customer's Demand | 145 |
| | Seven Steps to Creating a Data Sanitization Process | 145 |
| | Step 1: Prioritize and Scope | 146 |
| | Step 2: Orient | 146 |
| | Step 3: Create a Current Profile | 146 |
| | Step 4: Conduct a Risk Assessment | 147 |
| | Step 5: Create a Target Profile | 147 |
| | Step 6: Determine, Analyze, and Prioritize Gaps | 147 |
| | Step 7: Implement Action Plan | 147 |
| | Data Sanitization Defined | 147 |
| | Physical Destruction | 148 |
| | Degaussing | 148 |

| | |
|---|-----|
| Pros and Cons of Physical Destruction | 148 |
| Cryptographic Erasure (Crypto-Erase) | 148 |
| Pros and Cons of Cryptographic Erasure | 149 |
| Data Erasure | 149 |
| Pros and Cons of Data Erasure | 150 |
| Equipment Details | 150 |
| Asset Lifecycle Procedures | 151 |
| Suggested Process, In Short | 152 |
| Create Contract Language for Third Parties | 152 |
| Data Erasure Procedures | 152 |
| Responsibility | 152 |
| Validation of Data Erasure Software and Equipment | 153 |
| Personal Computers | 153 |
| Servers and Server Storage Systems | 154 |
| Photocopiers, Network Printers, and Fax Machines | 154 |
| Mobile Phones, Smartphones, and Tablets | 154 |
| Point-of-Sale Equipment | 155 |
| Virtual Machines | 155 |
| Removable Solid-State Memory Devices | |
| (USB Flash Drives, SD Cards) | 155 |
| CDs, DVDs, and Optical Discs | 155 |
| Backup Tape | 155 |
| General Requirements for Full Implementation | 155 |
| Procedure for Partners and Suppliers | 155 |
| Audit Trail Requirement | 156 |
| Policy Ownership | 156 |
| Mandatory Revisions | 156 |
| Roles and Responsibilities | 157 |
| <i>CEO</i> | 157 |
| <i>Board of Directors</i> | 157 |

| | |
|--------------|------------|
| Index | 159 |
|--------------|------------|