Contents

Dedication iii
About the Authors xv
   Sharon D. Nelson, Esq. xv
   David G. Ries, Esq. xvi
   John W. Simek xvii
Acknowledgments xix
Introduction xxi

1. Current Developments Affecting Law Firm Information Security 1
   What’s New in the Data Breach World? 1
   What New Developments Have Affected Law Firm Information Security? 2
   The Rise of Spear Phishing 5
   The Bad Rap Law Firms Get on Information Security Is Slowly Changing 6
   Okay, You’re Convinced: What’s Next? 8

2. Real-Life Law Firm Data Breach Nightmares 11
   Can Your Law Firm Be Breached? 11
   The Nonlawyer Breaches 12
   Law Firm Data Breaches 13
      2015: Atkinson, Andelson, Loya, Ruud & Romo 13
      2015: An Alleged Data Breach 14
      2014: Compromise of a Law Firm to Target Clients 15
      2014: Imhoff and Associates 16
      2014: Wilson Sonsini Goodrich & Rosati 16
      2014: Snowden Revelation of NSA Surveillance 17
      2013: McKenna Long & Aldridge 19
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012: Unknown New York Law Firm</td>
<td>19</td>
</tr>
<tr>
<td>2012: Puckett &amp; Faraj</td>
<td>20</td>
</tr>
<tr>
<td>2011: Wiley Rein</td>
<td>21</td>
</tr>
<tr>
<td>2011: Baxter, Baker, Sidle, Conn &amp; Jones</td>
<td>21</td>
</tr>
<tr>
<td>2008: An Unknown Law Firm</td>
<td>22</td>
</tr>
<tr>
<td>Conclusion</td>
<td>22</td>
</tr>
</tbody>
</table>

### 3. Lawyers’ Duty to Safeguard Information 23

- Ethical Duties Generally                                    23
- Ethical Duties: Electronic Communications                   32
- Common-Law Duties                                           36
- Statutes and Regulations                                    37
- Standards for Competent and Reasonable Measures              40
- Conclusion                                                  42
- Selected Ethics Opinions: Technology, the Internet, and     42
  Cloud Computing

### 4. Physical Security 45

- Introduction                                                45
- Where Is Your Server and Who Has Access to It?              45
- Alarm Systems, UPS, and Paper                                46
- Security Assessments                                        47
- Laptops                                                     48
- Lost and Stolen Devices                                     49
- Training                                                    49
- Guests                                                      50
- Incident Response Plans and Disaster Recovery Plans         51
- Physical Security Assessments                               51

### 5. Information Security Overview 53

- Security Frameworks and Standards                           54
- The NIST Cybersecurity Framework                            57
- The FTC Safeguards Rule                                     59
- ISO 27000 Standards                                         60
- NIST Standards                                              62
  - The NIST Small Business Guide                             62
- US-CERT Resources for Small and Midsized Businesses         64
- The Critical Security Controls                              64
- Strategies to Mitigate Targeted Cyber Intrusions            67
- The LegalSEC Top 10                                         67
- Five Common Failures in Network Security                    68
- The 80-20 Rule                                              69
- Security Programs and Policies                              69
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory and Risk Assessment</td>
<td>70</td>
</tr>
<tr>
<td>People</td>
<td>71</td>
</tr>
<tr>
<td>Policies and Procedures</td>
<td>72</td>
</tr>
<tr>
<td>Technology</td>
<td>73</td>
</tr>
<tr>
<td>Third Parties and Outsourcing</td>
<td>73</td>
</tr>
<tr>
<td>Incident Response</td>
<td>73</td>
</tr>
<tr>
<td>Threat Intelligence and Information Sharing</td>
<td>74</td>
</tr>
<tr>
<td>Defense in Depth</td>
<td>75</td>
</tr>
<tr>
<td>Conclusion</td>
<td>76</td>
</tr>
<tr>
<td>Technology Users Run Amok</td>
<td>77</td>
</tr>
<tr>
<td>Electronic Communications and Internet Use Policy</td>
<td>78</td>
</tr>
<tr>
<td>Social Media Policy</td>
<td>78</td>
</tr>
<tr>
<td>Document Retention Policy</td>
<td>79</td>
</tr>
<tr>
<td>Physical Security Policy</td>
<td>79</td>
</tr>
<tr>
<td>Secure Password Policy</td>
<td>80</td>
</tr>
<tr>
<td>BYOD, BYON, and BYOC</td>
<td>80</td>
</tr>
<tr>
<td>Disaster Recovery Plan</td>
<td>81</td>
</tr>
<tr>
<td>Mobile Security Policies</td>
<td>81</td>
</tr>
<tr>
<td>Equipment Disposal Policy</td>
<td>82</td>
</tr>
<tr>
<td>Incident Response Plans</td>
<td>82</td>
</tr>
<tr>
<td>The Elements of an IRP</td>
<td>83</td>
</tr>
<tr>
<td>7. Authentication and Authorization</td>
<td>87</td>
</tr>
<tr>
<td>“Why a String of Characters Can’t Protect Us Anymore”</td>
<td>88</td>
</tr>
<tr>
<td>Authentication</td>
<td>90</td>
</tr>
<tr>
<td>Something the User Knows</td>
<td>91</td>
</tr>
<tr>
<td>Something the User Has</td>
<td>94</td>
</tr>
<tr>
<td>Something the User Is</td>
<td>96</td>
</tr>
<tr>
<td>The Need for Multiple Factors</td>
<td>98</td>
</tr>
<tr>
<td>Multifactor Authentication—Some Examples</td>
<td>99</td>
</tr>
<tr>
<td>RSA SecureID</td>
<td>99</td>
</tr>
<tr>
<td>SecureAuth and Authentify, Multifactor Authentication Solutions</td>
<td>100</td>
</tr>
<tr>
<td>Google Two-Step Verification</td>
<td>100</td>
</tr>
<tr>
<td>Backup Phones and Codes</td>
<td>101</td>
</tr>
<tr>
<td>Google Authenticator App</td>
<td>101</td>
</tr>
<tr>
<td>Dropbox Two-Step Verification</td>
<td>101</td>
</tr>
<tr>
<td>Mobile Authenticator Apps</td>
<td>101</td>
</tr>
<tr>
<td>Emergency Backup Code</td>
<td>101</td>
</tr>
<tr>
<td>Apple’s iCloud Two-Step Verification</td>
<td>102</td>
</tr>
<tr>
<td>Recovery Key</td>
<td>102</td>
</tr>
</tbody>
</table>
Multifactor Authentication for Office 365 103
Other Services with Two-Factor Authentication 103
Conclusion 103

8. Encryption: Its Time Is Here 105
   Why Attorneys Need Encryption 105
   Encryption Overview 107
   Conclusion 111

9. Security Tools and Services 113
   Managed Security 113
   Incident Management 114
   Spam Filtering 114
      Blacklists and Whitelists 116
   Web Filtering 116
   Wireshark 117
   Nmap 118
   Penetration Testing Tools 119
      What Is Penetration Testing? 119
      Metasploit 121
      Pineapple Mark V 121
   Other Types of Security Assessments 122
   Client Security Assessments 123

10. Desktops, Laptops, and Servers 125
    Authentication 126
    User Accounts 126
    Secure Configuration 127
    Security Software 128
    Patching 130
    Hardware Firewall 131
    Encryption 131
       Disk Encryption Basics 132
       Encryption in Operating Systems 133
          Windows 133
          Apple OS X 135
       Encryption Software 135
       Laptops 136
       Desktops 136
       Servers 137
    Backup 137
    Installing Programs 137
    Safe Browsing 137
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachments and Embedded Links</td>
<td>139</td>
</tr>
<tr>
<td>Laptops</td>
<td>139</td>
</tr>
<tr>
<td><strong>11. Mobile Devices: Smartphones and Tablets</strong></td>
<td>143</td>
</tr>
<tr>
<td>Some Statistics</td>
<td>144</td>
</tr>
<tr>
<td>Attorneys' Duty to Safeguard Client Information</td>
<td>144</td>
</tr>
<tr>
<td>Mobile Security Basics</td>
<td>145</td>
</tr>
<tr>
<td>Smartphones and Tablets</td>
<td>146</td>
</tr>
<tr>
<td>Encryption: A Security No-Brainer</td>
<td>148</td>
</tr>
<tr>
<td>Additional Security Considerations</td>
<td>148</td>
</tr>
<tr>
<td>Additional Information</td>
<td>151</td>
</tr>
<tr>
<td><strong>12. Portable Storage Devices</strong></td>
<td>153</td>
</tr>
<tr>
<td>Encrypted USB Flash Drives</td>
<td>154</td>
</tr>
<tr>
<td>Encrypted External Hard Drives</td>
<td>157</td>
</tr>
<tr>
<td>Operating System Encryption of Portable Drives</td>
<td>157</td>
</tr>
<tr>
<td>Encryption Software</td>
<td>158</td>
</tr>
<tr>
<td>Enterprise Management</td>
<td>158</td>
</tr>
<tr>
<td><strong>13. The Internet of Everything</strong></td>
<td>159</td>
</tr>
<tr>
<td>Lawyers and IoE</td>
<td>160</td>
</tr>
<tr>
<td>IoE Devices: Their Rise and Their Shortcomings</td>
<td>161</td>
</tr>
<tr>
<td>Privacy</td>
<td>162</td>
</tr>
<tr>
<td>Security</td>
<td>162</td>
</tr>
<tr>
<td>Security Tips in an IoE World</td>
<td>164</td>
</tr>
<tr>
<td>The Future of IoE</td>
<td>165</td>
</tr>
<tr>
<td><strong>14. Secure Disposal</strong></td>
<td>167</td>
</tr>
<tr>
<td>The Issues</td>
<td>168</td>
</tr>
<tr>
<td>Solutions</td>
<td>169</td>
</tr>
<tr>
<td>Conclusion</td>
<td>173</td>
</tr>
<tr>
<td><strong>15. Digital Copiers</strong></td>
<td>175</td>
</tr>
<tr>
<td>Administration</td>
<td>175</td>
</tr>
<tr>
<td>Scanner</td>
<td>176</td>
</tr>
<tr>
<td>Fax</td>
<td>177</td>
</tr>
<tr>
<td>Disposal</td>
<td>177</td>
</tr>
<tr>
<td>Other Considerations</td>
<td>178</td>
</tr>
<tr>
<td><strong>16. Networks: Wired and Wireless</strong></td>
<td>179</td>
</tr>
<tr>
<td>Authentication and Access Control</td>
<td>179</td>
</tr>
<tr>
<td>Wired Networks</td>
<td>180</td>
</tr>
<tr>
<td>Wireless Networks</td>
<td>180</td>
</tr>
<tr>
<td>Firewalls/IDS/IPS Devices</td>
<td>184</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>186</td>
</tr>
</tbody>
</table>
Routers 187
Switches 188
Servers and Network Devices 189
Other Considerations 190

17. Remote Access 191
   Virtual Private Networking 192
   iTwin Connect 193
   Remote Control 193
   Remote Node 194
   Remote Authentication 194

18. E-Mail Security 195

19. Voice Communications 203
   Traditional Telephone Systems 203
   Voice over Internet Protocol (VoIP) Systems 204
   Voice Mail 205

20. Backup and Business Continuity 207
   Backup Job Types 207
      Full 208
      Differential 208
      Incremental 208
   Backup Media 208
   Backup Solutions 209
   Business Continuity 210

21. Outsourcing and Service Providers 213

22. Cloud Computing 217
   Definition 217
   The Ethical Side of the Cloud 218
   Developing Cloud Security Standards 224
   Encryption in the Cloud 227
   The Practical Side of the Cloud 228
   Conclusion 231

23. Social Media 233

24. Securing Documents 237
   Word 237
   Adobe Acrobat 238
   Document Management 240
   Compound Files 240
Contents

Metadata 241
Final Thoughts 242

25. Cyberinsurance 243
   Introduction 243
   How Much Does It Cost? 245
   What Will a Prospective Insurer Ask You? 247
   Coverage 249

   Security Certifications and Security Audits 255
   Policies and Plans 256
   Passwords and Multifactor Authentication 256
   Encryption 257
   Social Media 257
   Mobility 257
   File-Syncing Software—Dropbox and its Brethren 257
   Drone Cyber Attacks 258
   Information Rights Management 258
   Changing Focus to Detection, Response and Recovery 258
   Who You Gonna Call? Information Security Experts 259
   Final Words 259

27. Additional Information Resources 261
   Short List of Favorite Information Sources 261
   Top 50 InfoSec Blogs 263
   Further Resources 265
   Security Feeds 265
   Security Web Sites 266
   OS Feeds 270
   People Feeds 270
   Cloud 272
   Security News Feeds 272
   General Feeds 273
   Tools 274
   Information Sources: Professional Responsibility and
   Cloud Computing 277
   Mobile Security 279
   Online Resources 279
   Books 280
   Reports and Papers* 281
   Articles* 282
   Other Resources 283
# Contents

**Appendix A**  
Excerpts from ABA 2015 Legal Technology Survey Report 285

**Appendix B**  
Selected ABA Model Rules of Professional Conduct 301  
  - Rule 1.1: Competence 301  
    - Comment on Rule 1.1 301  
  - Rule 1.6: Confidentiality of Information 303  
    - Comment on Rule 1.6 303  
  - Rule 5.3: Responsibilities Regarding Nonlawyer Assistance 310  
    - Comment on Rule 5.3 311

**Appendix C**  
Pennsylvania Ethics Opinion—Cloud Computing 313

**Appendix D**  
California Ethics Opinion—Confidentiality and Technology 335

**Appendix E**  
New York Ethics Opinion—Remote Access 343

**Appendix F**  
Massachusetts Regulations—Personal Information Protection 347  
  - Massachusetts Regulations on Personal Information Protection 347  
    - 17.01 Purpose and Scope 348  
    - 17.02: Definitions 348  
    - 17.03: Duty to Protect and Standards for Protecting Personal Information 349  
    - 17.04: Computer System Security Requirements 351  
    - 17.05: Compliance Deadline 352

**Appendix G**  
FTC Safeguards Rule 353

**Appendix H**  
NIST Cybersecurity Framework (without appendices) 357

**Appendix I**  
NIST Small Business Information Security 377

**Appendix J**  
Lockdown: Information Security Program Checklist 409

**Appendix K**  
Federal Trade Commission: “Start With Security” 413
Appendix L 431
  Sensei Employee Out-Process Checklist 431

Appendix M 433
  Sample Security Policies for Smaller Firms 433
  Confidentiality Policy 433
  Personal Device Policy 434
  Information Security Policy 436
  Online Activity Policy 440

Appendix N 445
  FTC Disposal Rules 445

Appendix O 449
  SANS Institute Glossary of Security Terms 449

Appendix P 489
  Updates 489

Index 497