# Electronic Commerce: Security, Risk Management and Control

**Marilyn Greenstein, Ph.D.**
*Lehigh University*
*Bethlehem, Pennsylvania*

**Todd M Feinman**
*PricewaterhouseCoopers LLP*
*New York, New York*

Irwin
McGraw-Hill

Boston Burr Ridge, IL Dubuque, IA Madison, WI New York San Francisco St. Louis
Bangkok Bogota* Caracas Lisbon London Madrid
Mexico City Milan New Delhi Seoul Singapore Sydney Taipei Toronto

# CONTENTS


**1. OVERVIEW OF ELECTRONIC COMMERCE**

Introduction 1
Definition of Electronic Commerce 1
Electronic Business 2
Potential Benefits of Electronic Commerce 3
The Internet and WWW as Enablers of Electronic Commerce 6
Impact of Electronic Commerce on Business Models 8
Overall Business and E- Commerce Goal Congruence 9
The Impact of Electronic Commerce on the Value Chain 13
The ICDT Business Strategy Model 15
Three Pillars of Electronic Commerce 18
Electronic Commerce Security 20
Organization of Topics 22
Implications for the Accounting Profession 22
Summary 23
Keywords 24
Review Questions 24
Discussion Questions 25
Cases 25

**2. ELECTRONIC COMMERCE AND THE ROLE OF INDEPENDENT THIRD-PARTIES**

Introduction 27
Consulting Practices and Accountants' Independence 28
CPA Vision Project 29
New Assurance Services Identified by the AICPA 30
The Elliott Committee and the Cohen Committee 32
Three Waves of Electronic Commerce 34
Electronic Commerce Integrity and Security Assurance 35
Electronic Commerce Systems Reliability Assurance 36
Internal Control Framework 38
Competition 39
Risk Assessment Assurance 39
Impact of Electronic Commerce on the Traditional Assurance Function 40
Continuous Auditing 40
Third-Party Assurance of Web-Based Electronic Commerce 41
Security of Data 41
Business Policies 42
Transaction Processing Integrity 43
Privacy of Data 43
Web Site Seal Options 43
Better Business Bureau 44
Truste 45
Veri-Sign 46
ICSA 47
AICPA/CICA Webtrust 49
Business Practices 51
Transaction Integrity 51
Information Protection 53
Report Issuance 53
Comparison of Seals 53
Implications for the Accounting Profession 55
Skill Sets 55
Expansion of Assurance Services 56
Consulting and International Services 57
Summary 57
Keywords 58
Review Questions 58
Discussion Questions 59
Cases 60

**3. THE REGULATORY ENVIRONMENT**

Introduction 63
Cryptography Issues 64
Key Length 65
Key Escrow and Key Recovery 70
International Cryptography Issues 71
Privacy Issues 72
FTC Privacy Online Report 73
Adults' Privacy Rights and The EU's Directive 77
Web Linking 80
Inappropriately Referencing a Linked Site 80
Displaying Information without Proper Referencing 81
Linking Using Framing 81
Linking Using Trademark in Keyword MetaTags 81

Unauthorized Display of a Registered Trademark 82
Linking to Illegal Files 83
Domain Name Disputes 83
Similarly Named Companies or Products 86
Registering and Using a Competitor's Name 87
Domain Names Registered and Held Hostage 87
Domain Name Dispute Resolution 88
Internet Sales Tax 88
International Tax Issues 89
Electronic Agreements and Digital Signatures 90
Internet Service Prodivers and International Libel Laws 91
Implications for the Accounting Profession 92
Liability Exposure and Risk Assessment 92
Expansion of Legal Resources and Services 93
Digital Signatures and Certificate Authorities 93
Summary 94
Keywords 94
Review Questions 95
Discussion Questions 95
Cases 96

**4. EDI, ELECTRONIC COMMERCE, AND THE INTERNET**
Introduction 101
Traditional EDI Systems 101
The Origin of EDI 102
Non-EDI Systems 102
Value-Added Networks (VANs) and Preestablished Trading Partners 104
Partially Integrated EDI Systems 104
Fully Integrated EDI Systems 106
Benefits of EDI Systems 107
Data Transfer and Standards 109
Department of Defense Transaction Example 113
Financial EDI 113
EDI Systems and the Internet 116
Security Concerns 116
Security of Data during Transmission 117
Audit Trails and Acknowledgements 118
Authentication 118
Internet Trading Relationships 118
Consumer to Business 118
Business to Business 119
Government to Citizen 119
Benefits 120
EDI Web Browser Translation Software 123
Insight's EDI and Internet Systems 123
Real-time EDI Inventory Links with Suppliers 124
Integrated Delivery Links with Federal Express 124
Web-Based Sales 124
Impact of EDI-Internet Applications on the Accounting Profession 125
Increased Complexity of Auditing through the Computer 125
Integrity of and Reliance in the VANs 126
Extension of Audit to Trading Partners' Systems 126
Increased Technological Skills of Smaller Accounting Firms 126
Summary 127
Keywords 127
Review Questions 127
Discussion Questions 128
Cases 129

**5. RISKS OF INSECURE SYSTEMS**
Introduction 131
Overview of Risks Associated with Internet Transactions 132
Internet Associated Risks 135
Risks to Customers 136
False or Malicious Web Sites 136
Stealing Visitors' Ids and Passwords 136
Stealing Visitors' Credit Card Information 136
Spying on a Visitor's Hard Drive 136
Theft of Customer Data from Selling Agents and ISPs 137
Privacy & the Use of Cookies 137
Risks to Selling Agents 141
Customer Impersonation 141
Denial of Service Attacks 142
Data Theft 143
Intranet Associated Risks 143
Sabotage by Former Employees 145
Threats from Current Employees 147
Sniffers 148
Financial Fraud 149
Downloading of Data 150
E-Mail Spoofing 151
Social Engineering 151
Risks Associated with Business Transaction Data Transferred between Trading Partners 153
Intranets, Extranets and Internet Relationships 153

Data Interception 155
Message Origin Authentication 156
Proof of Delivery 157
Message Integrity & Unauthorized Viewing of Messages 157
Timely Delivery of Messages 157
Risks Associated with Confidentially-Maintained Archival, Master File and Reference Data 157
Risks Associated with Viruses and Malicious Code Overflows 159
Viruses 159
Trojan Horses 162
Hoaxes 163
Buffer Overflows 163
Implications for the Accounting Profession 163
Intranets and Internal Controls 164
Internet and Internal Controls 164
Web Site Assurance 165
Summary 165
Keywords 166
Review Questions 166
Discussion Questions 167
Cases 167

**6. RISK MANAGEMENT**
Introduction 171
Control Weakness vs. Control Risk 173
Security Gaps 174
Culture Management 174
Excessively Tight Controls 175
Risk Management Paradigm 176
Disaster Recovery Plans 178
Disaster Recovery Plan Objectives 178
Second Site Back-up Alternatives 180
Mutual Aid Pact 180
Cold Site/Crate and Ship 180
Hot Site 181
Conducting a Dress Rehearsal 181
Implications for the Accounting Profession 181
Evolution of Internal Control Framework 182
The Control Environment 183
Risk Assessment 184
Control Activities 185
Information and Communication 186
Monitoring 186
The Role of Internal Controls in Risk Management 186
Summary 188
Keywords 188
Review Questions 189
Discussion Questions 189
Cases 189

7. INTERNET SECURITY STANDARDS
Introduction 193
Standard Setting Issues and Committees 193
ANSI 195
UN/EDIFACT 195
ANSI's ASC XI2 Alignment Task Group Leading the Migration to UN/EDIFACT 196
Major Standard Setting Structures and Interfaces 196
U.S. and International Standard Setting Bodies 196
Internet and WWW Committees 198
Internet Committees 198
WWW Committees 200
W3C 200
OBI 200
Global Information Infrastructure Commission 201
Security Committees and Organizations 201
Security Protocols and Languages 202
OSI 203
TCP/IP 204
IP Addresses 204
Class A 204
Class B 205
Class C 206
fc Class D and Class E 205
Domain Names 206
IPv6 207
FTP and TELNET 207
NNTP 208
HTTP and HTTP-NG 208
S-HTTP, SSL, and PCT 208
SGML, HTML, and XML 209
DOM and DHTML 210
JAVA 212
STEP 213
Messaging Protocols 214
Basic Mail Protocols 214
Security-Enhanced Mail Protocols 216
Secure Electronic Payment Protocols 217
The Role of Accountants in Internet-related Standard Setting Process 219
Summary 219
Keywords 219
Review Questions 221
Discussion Questions 222
Cases 222

**8. CRYPTOGRAPHY AND AUTHENTICATION**
Introduction 227
Messaging Security Issues 227
Confidentiality 229
Integrity 229
Authentication 229

Non-Repudiation 230
Access Controls 231
Encryption Techniques 232
Symmetric Encryption Keys 233
Data Encryption Standard 233
Triple Encryption 234
Advanced Encryption Standard 235
Skipjack 235
RC2, RC4, and RC5 235
Asymmetric Cryptography 235
Public-Private Key Pairs 237
Elliptic Curve Cryptography 241
Integrity Check Values and Digital Signatures 241
Integrity Check Value (Hashes) 242
Digital Signatures 243
One Time Pads 246
Good Encryption Practices 246
Password Maintenance 246
Key Length 247
Key Management Policies 247
Compressed Files 247
Message Contents 247
Key Management 248
Public Certification Authorities 250
Private or Enterprise Certification Authorities 252
Hybrid Public and Private Certification Authorities 252
Key Management Tasks 252
Identification and Verification of Users 253
Key Generation 253
Key Registration 253
Key Escrow and Recovery 253
Key Updates and Replacement 253
Key Revocation and Destruction 253
Additional Authentication Methods 254
Additional Non-Repudiation Techniques 256
Implications for the Accounting Profession 256
Confidentiality 256
Message Integrity 257
Authentication 257
Non-repudiation 258
Access Controls 259
Internal Control and Risk Analysis 259
Summary 259
Appendix A - The RSA Algorithm 260
Appendix B - XOR Function 260
Keywords 261
Review Questions 262
Discussion Questions 263
Cases 263

**9. FIREWALLS**

Introduction 267
Firewall Defined 268
TCP/IP 269
Open Systems Interconnect (OSI) 269
Components of a Firewall 270
Typical Functionality of Firewalls 272
Packet Filtering 274
IP Spoofing 274
Network Address Translation 275
Application-Level Proxies 275
Stateful-Inspection 278
Virtual Private Networks 279
Real-Time Monitoring 279
Network Topology 280
Demilitarized Zone 281
Securing The Firewall 282
Policy 282
Network Security Access Policy 282
Firewall Design Policy 283
Administration 283
Services 284
Telnet and FTP Security Issues 284
Finger Service Security Issues 285
Internal Firewalls 285
Authentication 286
Operating System Controls 286
Factors to Consider in Firewall Design 286
In-House Solutions vs. Commercial Firewall Software 287
Limitations of the Security Prevention Provided by Firewalls 288
Implications for the Accounting Profession 289
Penetration Testing and Risk Exposure 289
Provider of Network Solutions 290
Forensic Accounting and Intrusion Investigation 290
Summary 290
Keywords 291
Review Questions 291
Discussion Questions 292
Cases 292

**10. ELECTRONIC COMMERCE PAYMENT MECHANISMS**

Introduction 295
The SET Protocol 295
SET vs. SSL 297
Version 1.0 298
Payment Gateway 298
Certificate Issuance 299
Certificate Trust Chain 299
Cryptography Methods 299
Dual Signatures 300
The SET Logo 302
Compliance Testing 302
Status of Software Implementations 304

Version 2.0 and Intermediate Releases 304
Magnetic Strip Cards 305
Smart Cards 308
Electronic Checks 312
The FSTC's Electronic Check 316
The FSTC's BIPS Specification 318
BJPSandEDI 320
Electronic Cash 320
Implications for the Accounting Profession 321
Audit Implications 322
Electronic Bill Presentment and Payment Systems 322
Summary 322
Keywords 323
Review Questions 323
Discussion Questions 324
Cases 324

**11. INTELLIGENT AGENTS**
Introduction 329
Definition of Intelligent Agents 329
Capabilities of Intelligent Agents 331
Level of Agent Sophistication 334
Agent Societies 335
Intelligent Agents & Electronic Commerce 337
The Online Information Chain 341
Push Technology and Marketing 342
Pull Technology and Demands of Information and Services 342
New Geographical Markets 345
Business-to-Business Transaction Negotiation 345
Limitations of Agents 346
Implications for the Accounting Profession 347
Continuous Reliability Assurance 347
Agents and Security 348
Summary 348
Keywords 348
Review Questions 349
Discussion Questions 350
Cases 350

**12. WEB-BASED MARKETING**
Introduction 353
The Scope of Marketing 353
Business, Marketing, and Information Technology Strategy Congruence 354
The Four Ps Applied to Internet Marketing 358
Product 359
Pricing 360
Place (Distribution) 361
Promotion 362
The Fifth "P" - Personalization 364
Toffler's Powershift 365
Marketing Implications of the Consumer Power Shift 366
Building Relationships through Database Marketing 366
Personalized Transaction Domain 366
The Relentless Search for Value 367
Internet Marketing Techniques 367
Passive Providers of Information 368
Search Engine and Directory Registration 370
Solicited, Targeted E-mail 370
Interactive Sites 370
Banner Advertising 371
Off-Line Advertising 371
Unsolicited, Targeted E-Mail 372
Spam Mail 372
E-mail Chain Letters 373
On-Line Advertising Mechanisms 373
Directories 373
Search Engines 376
Keywords and Meta Tags, and Frequency of Words 376
Location of Words 377
Link Popularity 377
w Reviewed Sites 377
Case Sensitive 378
Banners 377
Sponsorships 379
Portals 379
On-line Coupons 380
Web Site Design Issues 381
Page Loading Efficiency381
Simplicity 381
Use the Space Wisely 381
Create a Reason to Return 382
Framing 382
Tables and Fonts 382
Graphics 382
Interlaced Graphics 382
GIF vs. JPEG Files 383
Colors and Contrast 383
Purchasing Information 383
Tracking Data 384
Intelligent Agents and Their Impact on Marketing Techniques 384
Implications for the Accounting Profession 385
Summary 385
Keywords 386
Review Questions 386
Discussion Questions 387
Cases 387

INDEXES 391