Index

access control using
  password and PIN, 121–22
  tokens and smart cards, 122–23
access devices, 19
account aggregator, 22
Advantage mortgage, 31
aggregation, 21
aggregator, 19, 21–22, 60
AIG debacle, 60–61, 161–62
alternate system of trading, 109–10
Application Programming Interface (API), 23
Application Service Provider (ASP), 41–42
asymmetric cryptography, 125, 146–47
asymmetric key encryption, 124–26
automated scanning tools, 129
automated teller machine (ATM), 37, 43, 83

Bankers' Book of Evidence Act, 1891, 112, 115–16, 141, 146, 156–57
Bank for International Settlement (BIS) guidelines for risk management, 99, 104–05, 114
Basel Committee on Risk for Electronic Banking, 91, 100–01, 106
biometrics authentication techniques, 123
black hackers, 94
Bombay Stock Exchange, 66, 71
book store effect, 78
Brick and Click model, 5, 13, 18, 28, 40, 56, 65, 74–89, 175
business planning, integration with marketing, 78–80
Business-to-Consumer (B2C) segment, 31

card-based scheme, 30
Carnegie Mellon Software Engineering Institute Network Systems Survivability Program, 131
certification authority (CA), for digital signatures, 148–50
Civil Procedure Code, 141
Clearing Corporation of India, 10, 67, 71–73
click and brick marketing, *See* marketing
Code of Criminal Procedure, 112
configuration issues, 133
connectivity risks, 108
control devices, in network security, 121–23
corporate plans, marketing plan in, 79–80
cracker, 112
credit risk, 90–91
Cryptographically Strong Pseudo Random Number Generator (CSPRNG), 126
cryptographic keys, 113
customer service, 5, 29, 35, 39, 74, 76
cyber crime, 111–17
  effects, 114
  enforcement problems, 115–17
  forms, 112
  IT Act and, 113–14
  real and hearsay evidence, 115
  reasons, 112–13
cyber laws
  contract aspect, 144–45
  evidence aspect, 149–57
  functional equivalent approach, 145–49
  intellectual property aspects, 158
  jurisdiction, 143–44

data systems incompatibility, 108
data transmission reliability, 124
denial of service attacks, 129, 132
digital signatures
  certification, 148–50
  creation of, 147
  definition, 146
due diligence, and risk, 100, 105, 172

e-banking, 22–24, 37–59
  access to, 37
  ASP selection, 42
  bankers perception, 38
  bank websites, 42–45
  B2B applications, 48
  definition, 37
  differentiation aspect, 52–53
  efficacy evaluation, 52
  impact assessment, 50–51
  internet and non-internet banks, 56
  mobile banking, 58–59
  objectives, 46
  planning and development, 39–45
  problems encountered, 22–24, 39
  products and services offered, 46–47
  risks
    BIS recommendations for management, 99, 104–06
    conduct of business, 108–09
    connectivity, 108
    data security, 108
    factors, 53–54
    management, 104–10, 164–65
    operational, 107
    transaction, 107–08
  security measures, 109–10
  to small- and medium-sized enterprises, 49–50
  stand-alone e-banking, 54–58
  strategic risks, 106–07
  structural deficiencies, 107
  systems and services management, 137–40
e-broking, 162–66
  client-broker relationship, 163–64
  contract notes, 165
  cross trades, 165–66
  operational and system requirements, 163
  risk management, 164–65
  STP framework, 165–66
e-commerce, *See also* e-banking
attendant risks, 108–09
Economic Cycle Reserve, 92
e-finance
  competition and cost savings, 15–16
  cost savings, 15
  delivery channels, 10–16
  enabling services and their importance, 8
  institutions regulation, 159–62
  internet pervasiveness and, 14–15
  IT as infrastructure technology, 12–14
  problems associated with, 19–20
  returns on IT investments, 11–12
  service, 37
  transition to, 7
e-finance institutions
  competition policy, 170–71
  e-broking, 162–66
  insurance sector, 166–68
  investor information and complaints, 164
  management oversight
    and due diligence, 172
    security controls, 171–73
  monetary policy implications, 168–70
  operational integrity, 163
  order/trade confirmation, 164
  personnel and procedures, 163
  regulation, 159–62
  regulatory contents, 161–62
  risk management principles, 172
  signature verification and authentication, 163
  smart and debit cards, 170
  system capacity, 163
e-insurance, 59–62
  risk management for, 104–10
electronic fund collection, through e-trading, 69–70
electronic system, and risk, 94
e-money, 30–32
encryption attacks, 132
e-procurement, 33–36
e-purse schemes, 30
equity markets, e-trading in, 33
e-security, in wireless network, 131

ethical hackers, 94
e-trading, 63–73
  advantages, 64–65
  electronic fund collection, 69–70
  in equity markets, 33
  in fixed-income securities, 70–72
  in foreign exchange, 72–73
  indicative or tradable, 68
  pre-trade transparency, 68–69
  price quantity real-time or delayed, 68–69
  services, 64
  in shares, 69
  systems, 33
  transparency, 67–69

Federal Deposit Insurance Corporation (FDIC), 39, 171–73
  guidelines, 93–94, 99, 101, 105
Financial Market Directive (MIFID), European Union, 67–68
firewall, 126, 128
fixed-income securities, e-trading in, 70–72
floor-based trading, 64
foreign exchange trading, 33, 72–73
fraudulent data misuse, 94

General Packet Radio Service (GPRS) vulnerability, 135
Grameen Bank, Bangladesh, 7, 33
Gray bank, e-banking at, 44
Groupe Spécial Mobile (GSM)
  and network security, 134–37
  security solutions for, 136–37
  vulnerability
    GPRS, 135
    SIM cards, 134–35
    SMS, 135–36
    WAP weaknesses, 136

hackers, 43, 94, 97–98, 112–13, 120, 122, 132
hedge funds, 92

IDS alert notifications, 129
I-Flex solutions, 41–42
incident response, in network security, 129–30
Indian Contract Act, 141
Indian Evidence Act 1872, 112, 115, 141, 146, 150–56
Indian Penal Code, 1860, 112, 146
information security risk assessment, 95
Information Technology (IT) Act, 2000, 112–13, 115, 141, 145–46, 149–56
in-house work done, 24–26
insertion attacks, 132
Insurance Regulatory and Development Authority (IRDA), 35, 59, 61, 166
insurance sector, 106, 166–68
intangible products marketing, 77–78
Intellectual Property Rights (IPR), 116, 158
International Association of Insurance Supervisors, 106, 166–68
internet
  banking, *See* e-banking
  characteristics, 4
  economics, 175–78
  enabled insurance, 61–62
  evolution, 2–4
  impact assessment, 5–7
  interaction and personal interaction, 176
  and non-internet banks dynamic analysis, 55–56
  objectives, 175
  pervasiveness and e-finance, 14–15
  potential, 174–78
  trading, *See* e-trading
  for underdeveloped countries, 7
  users growth, 2–3
Internet Protocol (IP) spoofing, 98
internet services
  clean slate approach, 29
  continual evolver approach, 28–29
  e-money, 30–32
  e-procurement, 33–36
  e-trading, 33, 63–73
  factoring and leasing, 32–33
  problems associated, 28
  reasons retarded developments of, 27–28
  traditional migrator approach, 28
intrusion detection systems (IDS), 95, 127

key encryption, 122, 125–26

liquidity
  regulation, 92
  risk, 90–91

majeure risks, 103
malicious attacks, and network security, 123–24
Management Information System (MIS), 49
management oversight
  and due diligence, 172
  of risks, 100, 105
  security controls, 171–73
managers' check list
  in marketing, 85–86
  for network security, 127–29
market
  risk, 90–91
  turbulence, 87–88
marketing, 76–88
  customers and, 76, 84–86
  grievance redressal, 87
  intangible products, 77–78
  integrating with business planning, 78–80
  managers' check list, 85–86
  market turbulence, 87–88
  max-e-imperatives, 84–85
  objectives, 80–85
  plan in corporate plans, 79–80
  strategy evaluation, 86–87
  supplier reach, 82–83
market would take care approach, 92–93
micro finance agencies, 49
mobile banking, 58–59
mobile node to mobile node attack, 133
Mobitrack service, 66
Model Law on Commercial Arbitration, 145–46
Multilateral Trading Facilities (MTFs), 67–68

National Infrastructure Protection Center (NIPC), 131
National Stock Exchange, 10, 71
Negotiated Dealing System of RBI, 70
network security, 118–40
  access control using
    password and PIN, 121–22
    tokens and smart cards, 122–23
  asymmetric key encryption, 125–26
  best practices in use, 128–29
  control devices, 121–23
  data transmission reliability, 124
  e-banking systems and services, 137–40
  e-security, 131
  failures, 119–21
  GSM and, 134–37
  incident response, 129–30
  malicious attacks, 123–24
  managerial checklist, 127–29
  manager's laptop problem, 132–33
  random numbers use, 126–27
  survivable system development, 130–31
  war driving, 132–34, 136
  wireless networks, 131–33

online client interface categories, 18
on-line payment systems, 169
online trading, implementation stage difficulties, 22–24
online value chain, 19–21
operational
  integrity, 163
  risk, 90–91, 107
organizational control, risk beyond, 102–03
outsourcing, 24–26
  e-finance systems and services management, 137–40
  risk of, 102

password
  access control using, 121–22
  generation, 121
  theft, 98, 112
penetration
  analysis, 95
  testing, 126
personal digital assistant (PDA), 37, 43
personal identification number (PIN), access control using, 121–22
pre-trade transparency, in e-trading, 68–69
Project Entropia, 30–31

pseudo-random number generators (PRNG), 126
pseudo-random numbers (PRN), 126
public key infrastructure (PKI) system, 128

random numbers, use in network security, 126–27
RBI Act of 1934, 141, 146
regulatory framework, for telecommunication, 8–9
Reserve Bank of India (RBI), 70–72, 74, 99, 160, 170–71
risk
  analysis, 90–91, 105
  assessment, 95–97
  beyond organizational control, 102–03
  conduct of business, 108–09
  connectivity, 108
  data security, 108
  due diligence, 100, 105, 172
  electronic system, 94
  elements, 90–91
  institutional and geographic regulation, 92–94
  management
    aspects, 90–103
    Basel committee and, 100–01, 106
    BIS guidelines, 99, 104–06
    for e-banking and e-insurance, 104–10
    FDIC guidelines, 93–94, 99, 101, 171–72
    mechanism, 99
    oversight, 100, 105, 171–73
    principles, 100–01, 172
  operational, 90–91, 107
  of outsourcing, 102
  potential threat, 97–100
  preventive measures, 94–95
  security controls, 100–02, 105, 171–73
  strategic, 106–07
  transaction, 107–08
  Turner recommendations to manage, 91–92
  vulnerabilities, 96–97
RSA asymmetric cipher, 125

Scare Socket Layer (SSL) protocol, 125–26, 136
securities, e-trading in, 33
Securities and Exchange Board of India (SEBI), 65, 69, 71–73, 109–10, 162–63, 165
security controls and risk, 100–02
security failures, 119–21
self-help groups (SHGs), 49
shares, e-trading in, 69
short message services (SMS) vulnerability, 135–36
signature verification and authentication, 163
Simple Network Management Protocol (SNMP), 128
small- and medium-sized enterprises, e-banking to, 49–50
smart cards, 170
  access control using, 122–23
sniffing, 113
social engineering, 98, 113
South Africa's Standard Bank, 32
stand-alone e-banking, 54–58
State Bank of India, 34
stealers, 112
strategic risks, 106–07
subscriber identification module (SIM) card vulnerability, 134–35
supplier reach, in marketing, 82–83
survivable network security system, development of, 130–31
Swedish Financial Supervisory Authority, 30
symmetric key encryption, 124

telecommunication, regulatory framework for, 8–9
telenet, 128
telephone-based trading, 64
threat, to computer security, 97–100
tokens, access control using, 122–23
trading, *See also* e-trading
  alternate system, 109–10
traffic interception and monitoring, 132, *See also* war driving
transaction risks, 107–08
transparency, in e-trading, 67–69
Trojan horses, 98–99, 123–24

Uncitral Model Law, 115, 149
United Nations Commission for Contracts for International Sale of Goods, 146, 149

VAR measures, 91
virtual private networks (VPN), 126, 136–37
viruses, 99, 129
voice-over IP, 129
vulnerabilities
  assessment tools, 95
  risk assessment and, 96–97

war dialing, 98, 133
war driving, 132–34, 136
websites
  access devices, 19
  aggregator, 21–22
  attacks on, 43–45
  design strategy, 20–21
  development of, 17–18
  e-banking, 22–24, 42–45
  online trading, 22–24
  online value chain, 19–21
  outsourcing and doing it yourself, 24–26
  portals, 19, 21–22
weightless economy, 77
wide area network (WAN), 137
Wireless Application Protocol (WAP) weaknesses, 136, 165
Wireless Equivalent Protocol (WEP), 132
Wireless Markup Language (WML), 136
wireless network (WLAN), e-security in, 129, 131–33
Wireless Transport Layer Security (WTLS), 136
Worms, 123–24