

Index

A

Advanced Encryption Standard (AES) 141
Australian Automotive Industry 145
authentication 162

B

B2C (business-to-consumer) transaction 98
biometric devices 96
Bluetooth 21
business practice security 21
business-to-business 118
business-to-business (B2B) transaction 98
business-to-consumer 118

C

China 98
clickstream tracking 95
client expertise 57
client privacy 53
client rights 53
closed system 114
commerce risk 112

commerce security 112
competitive advantage 117
confidentiality 162
consumer/client protection 24
continuity plan 5
continuous learning approach 59
corporate and government databases 91
credit reporting agencies 107
cyber risk 101
cybercrime 126
cybersecurity 127
Cyberterrorism Preparedness Act of 2002 81

D

data encryption standard (DES) 141
data integrity 162
demilitarized zone (DMZ) 142
digital certificate 30
digital content forum chair (DCF) 15
digital economy 135

E

e-commerce 89, 98, 113, 146
E-commerce adoption 146

- e-commerce initiatives 2
- e-commerce security 2, 135
- e-commerce security and the Law 122
- e-commerce security planning 158
- e-commerce skilled personnel 38
- e-commerce technologies 1
- e-commerce trust infrastructure 161
- eavesdropping 16
- electronic agreement 26
- employee education 164
- encryption 28

F

- file scans 17
- financial information databases 92
- financial pressure 64
- fireblock 83
- firemarshal 84
- firewalls 17, 118
- formal e-commerce security policy 12
- fraud 124

H

- hackers 16
- hacking 124, 128
- hacking techniques 64
- hands-on management 60
- hardware 4
- hardware watermarks 96
- honey-pots 142

I

- identity theft 128
- information security technologies 3
- intellectual property 129
- intentional destruction 5
- internal network infrastructure 160
- Internet investment 3
- Internet security field 77
- Internet security marketplace 78
- interoperability 41

L

- loss of technology 5
- loss of utilities 5

M

- man in the middle attacks 138
- management support 57
- management training 59
- medical information databases 93
- Microsoft SQL server 19
- modus operandi 140

N

- non-prime number keys 138
- non-repudiation 162

O

- online merchandise 123
- online trading 100
- open system 114
- OpenSource solutions 50
- Organisation for Economic Cooperation and Development 126
- organizational information technology resources 3

P

- PacketHound 81
- Palisade Systems 78
- personal information privacy 88
- predictability 115
- private key system 138
- public key infrastructure (PKI) 22

R

- real-time response teams 48
- regulatory framework 104
- resource constraints 103
- retention programs for personnel 40
- returns in investment 48
- risk and security management (RSM)

S

- ScreenDoor 80
- secure electronic transaction (SET) 6
- secure payment 35
- Secure Socket Layer (SSL) 6
- security architecture 20
- security breach 2
- security management 16
- self healing tools 142
- self-hosting 61
- self-regulation 32
- short message expansion 138
- SmokeDetector 83
- software applications security 21
- software watermarks 96
- status quo 140
- strategic plan for e-commerce security
6
- system security architecture 20

T

- tangible assets 114
- theft 5
- top management 13
- total e-commerce security program 4
- total security environment 45
- trading partners 153
- traffic 5
- transmission medium 154
- trust 145

U

- underdeveloped security controls 103

V

- vendors 5
- Verisign 24
- virtual assets 114
- virus attack 48
- volatility 115
- vulnerabilities 163

W

- weak technological support 102
- Web server threats 58
- Web-based businesses 125
- wired systems security 21
- wireless communications 94
- World Trade Organization (WTO) 99