Index

A
access control mechanisms 64
access point 112
administrative security policies 35
antivirus protection software 63
authentication 3, 122

B
biometric identifier 101
broadcast SSID 127
business impact 81
business-to-business relationship 42

customer base 47
customer litigation 58
customer provided information 42
customer relationship management (CRM) 46
customer-to-business relationship 42
cyber attacks 1

data encryption 3
data warehouse 4
denial of service (DoS) 3, 44, 121
deterrence-based trust 89
digital information 91
disaster recovery 67
disaster recovery plan 59
disaster recovery planning 104
“Do Not Call” list 11
dynamic host configuration protocol (DHCP) 127

e-business 67
electronic data interchange (EDI) 46
employee monitoring 34
encryption mechanism 65

Copyright © 2004, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
enterprise architecture 18, 27
enterprise resource planning (ERP) 46
external access points 98

F
Federal Trade Commission 10
firewall 1, 63
friction points 99

G
gateway systems 9
Government Information Security Reform Act 15

H
hacker 53, 117
hacking 8
hierarchy of controls model 74

I
identification-based trust 90
identify theft 11
identification of scope 79
information architecture 96
information assets 4
information assurance 22, 56
information loss 10
information security 34, 96
information systems 4
information transfer 9
infrastructure security plan 60
instant messaging (IM) 34
integrity 122
internal threat 54, 102
Internet protocol (IP) 3
Internet-related fraud 10
intrusion detection systems (IDS) 64
ISO security architecture 21
IT risk management 67

K
key risk areas 79
knowledge-based trust 89

L
LAN-jacking 117
legal responsibility 57
liability issues 2
litigation 11

M
measure compliance 86
multi-layer protection barriers 100

N
nDosa 129
network disconnect devices 65
networked system exploitation 53

P
packet sniffing 65
password 127
password controls 3
password sharing 10
privacy 2, 22
public key infrastructure (PKI) 91
public networks 9

R
risk assessment 56
risk assessment process 78
risk identification 78
risk management model 76
risk management success 69

S
security 116
security architectures 96
security audit 36
security enclave 62
security failures 42, 44
security incident reporting 48
security infrastructure 51
security mechanism 54
security policies 37
security program management 15
security standards 9
security strategies 1
service level agreements (SLAs) 98
shareholder wealth 44
small office/home office (SOHO) 110
software management servers (SMS) 63
software patches 9
SSID 112
standardized security processes 98
supply chain 42
support organizations 8
system-wide attacks 2

T
theft 2
threat matrix 97
Trojan horses 9
trusted partners 3
trusted systems 87

U
unauthorized access 10

V
virtual private network (VPN) 51
virus 44
viruses 2
vulnerability 43
vulnerability assessment 83

W
war chalking 117
war dialing 117
Web portals 6
Wi-Fi 112

Wi-Fi protected access (WPA) 112
wired equivalent privacy (WEP) 112, 121
wireless encryption protocol 126
wireless information security 110, 144
wireless local area network (WLAN) 112
worms 2