

Index

- 419 scams 162–3
- acceptable use policies (AUP) 47–53
- access control lists (ACLs) 250
- access privileges 9, 147–8, 250
- AccessEnum 250
- ACLs *see* access control lists
- Acrobat 198
- activation of software 197–8
- acunetix.com 138
- AdAware 189
- address verification service (AVS) 322
- administrator accounts 143, 147–8
- administrator passwords 35, 72–4
 - data interception 298
 - outsourcing 335, 337
 - server security 91–2
 - social engineering 316–17
 - temporary permissions 74–5
- Adobe Acrobat 198
- ADSL *see* asynchronous digital subscriber line
- Advanced Encryption System (AES) 255, 257–8
- adware 185–90, 275, 321
- AES *see* Advanced Encryption System
- Ameritrade 254
- antispam systems 154
- antivirus software 4
 - awareness training 59–60
 - computer faults 178, 179–80
 - heuristics 180–1
 - infected machines 176, 178–9
 - off-site computers 274
 - risk analysis 18, 21–2
 - shortcomings 177–81
 - signature databases 180–1
 - System Restore 181
 - testing 181–2
 - updates 179
- AOL 167–8
- archives 221–3
- Art of Intrusion, The* (Mitnick) 315
- asset control registers 26
- asset labels 372
- asymmetric encryption *see* public key encryption
- asynchronous digital subscriber line (ADSL) 275–6
- ATM machines 311–12
- attachments 156–8, 177
- AUP *see* acceptable use policies
- Austen, John 8, 11
- authentication
 - cookies 122
 - domain controllers 72–3
 - e-commerce fraud 319–26
 - phishing attacks 160–1
 - three principles 39–41

- author.exe 144
- autoresponder programs 56
- AVS *see* address verification service
- awareness training 18, 26, 55–63
 - class sizes 56–7
 - content 59–61
 - record keeping 62
 - senior management 61–2
 - session format 58–61, 62
 - technical knowledge 56–7
 - Web resources 62
- BAA *see* British Airports Authority
- BABS *see* British Airways Booking System
- back doors 175
- Back Orifice 102, 175
- backups 209–25
 - archives 221–3
 - awareness training 60
 - data 210
 - data recovery 220–1
 - encryption 253–4, 264
 - enterprise-level 219–20
 - frequency 213
 - full system 210, 219
 - hardware theft 370
 - internet-based 215–16
 - media 212–13
 - obsolescence 217–18, 223
 - restore process 217–19
 - retention 216–17
 - shortcuts 223–4
 - storage 213–15
 - strategies 209–11
 - Web sites 110–11, 120
- Baseline Security Analyzer (MBSA) 22, 68–9, 137, 179
- basic HTTP authentication 112–13
- BBC *see* British Broadcasting Corporation
- BCP *see* business continuity planning
- Best Practice Analyzer 137
- bin-raiding 93, 322
- biometrics 41–4
- BIOS pages 77
- Black Hat Briefings 258–9
- blackmail 17, 244
- Blaster virus 180
- blogs 232–3
- BlueTooth 129, 249
- boot options 77
- bots 174–5, 286–7
- British Airports Authority (BAA) 116
- British Airways Booking System (BABS) 255–6
- British Broadcasting Corporation (BBC) 261
- British Standards
 - BS7799 23, 25–7
 - BS7858 245
 - BS18044 365
- broadband 275–6
- browser caches 353–4
- browser plug-ins 188
- brute force attacks 114
- Brutus 114
- business continuity planning (BCP) 16, 359–67
- cache cleaners 348
- Caesar, Julius 268
- Caesar Cipher 142
- Caller ID 170
- Captain Crunch 159
- card security code (CSC) 322
- card verification number (CVN) 322
- cardholder not present (CNP)
 - transactions 319–26
- cash machines 311–12
- Central Intelligence Agency (CIA) 110
- Certification Authorities 270
- chat rooms 52, 169, 232, 273, 283
- checksum programs 111, 219

- child pornography 27–8, 228, 351
- Chip and PIN 322–6
- CIA *see* Central Intelligence Agency
- Cisco Systems 258–9
- CitiFinancial 254
- client-side code 120
- Clinton, Bill 110
- Cloudmark 167
- cmd.exe 144
- CNP *see* cardholder not present
- co-location facilities 1
- Communications Act 126–7
- communications data 111
- completewhois.com 103
- complexity requirements 33–4
- Computer Crime Unit 8, 11
- computer misuse 345–7
- Computer Misuse Act 2, 23, 24–5, 138
- confidence tricks *see* social engineering
- confidential information 29, 245
 - database-driven Web sites 118–19
 - encryption 261, 265
 - forensics 346
 - off-site computers 303–4
 - penetration testing 134
 - physical access 237, 342
 - redundant hardware 85–6
 - search engines 283–4
 - social engineering 312
 - see also* data theft
- confidentiality agreements 26
- content management systems 110, 119
- content scrambling system (CSS) 260
- cookie-poisoning 122
- CoolWebSearch 188
- Counterpane 335
- covert monitoring 350–1
- crack programs 200
- crackers 145
- cracking passwords 36–7
- cramm.com 13
- credit card fraud 118, 160–1, 319–26
- crossword solvers 39
- Crypto AG 257
- CSC *see* card security code
- CSS *see* content scrambling system
- Ctrl+Alt+Delete 75–6, 80, 185–6
- cuckoo sites 233–4
- curricula vitae (CVs) 245
- customer confidence 11, 14
- Cuthbert, Daniel 138
- CVN *see* card verification number
- CVs *see* curricula vitae
- Cybersource 325–6
- cybersquatting 115–16
- data
 - corruption 19, 20
 - interception 295–9
 - packets 101
 - recovery 220–1
 - retention 29–30
 - theft 243–51
 - wiping 85–6
 - see also* backups
- Data Encryption Standard (DES) 255, 257–8
- Data Protection Act 27, 29
- Data Protection Manager (DPM) 218, 219–20
- database servers 218
- database-driven Web sites 110, 116–20
- DDoS *see* distributed denial of service
- de Bernieres, Louis 261–2
- DeCSS 260
- defacement 110–11
- default accounts 78–9, 143, 147–8
- default passwords 35–6
- defeatingthehacker.com 4, 285–6
- deleted files 354–5
- demilitarized zones (DMZ) 104

- denial of service (DoS) attacks 285–8
 - accidental 287–8
 - firewalls 107
 - legislation 24
 - penetration testing 133
 - protection 287
 - viruses 173, 174–5
- DES *see* Data Encryption Standard
- DeviceLock 249, 303
- DeviceWall 249, 303
- diallers 192–3
- dictionary attacks 36–7
- Digital File Check 207–8
- digital rights management (DRM) 198, 205
- digital signatures 266
- digital subscriber line (DSL) 275–6
- disaster recovery planning (DRP) 16, 359–67
 - error messages 366
 - facilities 363–4
 - incident response 365
 - information security policy 49
 - insurance 360–1
 - maintenance 364–5
 - premises 361–3
 - prioritization 361
 - staff 363
 - testing 364–5
- disk quotas 82–3
- disposal of hardware 52
- distributed denial of service (DDoS)
 - attacks 286–7
- DivX files 205, 207
- DMZ *see* demilitarized zones
- DNS *see* domain name service
- document security 237–41
- domain controllers 73
- domain name service (DNS) servers
 - 89–90, 162
- domain names 114–16
- domain-based networks 4, 72–3
- DoS *see* denial of service
- DPM *see* Data Protection Manager
- Dr Solomon’s Antivirus Toolkit 214
- Draper, John 159
- DRM *see* digital rights management
- DRP *see* disaster recovery planning
- DSL *see* digital subscriber line
- dumpster diving 93, 322
- duress password 42–3
- DVD drives 212
- DVD format 260
- dynamic IP addresses 103
- e-commerce fraud 319–26
- Ebay 228
- Ebox Pro 117
- Edinburgh, Duke of 10–11
- EFS *see* encrypting file system
- EICAR *see* European Institute for Computer Antivirus Research
- Electronic Communications Act 27
- email 153–64
 - 419 scams 162–3
 - address allocation 168
 - attachments 156–8
 - awareness training 59–60
 - data interception 295–9
 - data theft 247–8
 - digital signatures 266
 - encryption 265–7
 - file extensions 83–4
 - forensics 346
 - headers 155–6
 - HTML/RTF formats 156–7, 159
 - information security policies 50
 - integrity 265
 - legislation 28–9
 - monitoring 163–4
 - non-repudiation 265–6
 - off-site computers 303

- personal 163–4
- pharming 161–2
- phishing attacks 158–61
- risk analysis 18
- scrambling 265
- spoofed 154–6
- viruses 177
- see also* spam
- emergency procedures 331
- EnCase 349–50, 353
- encrypting file system (EFS) 74, 262–5, 266–7, 303–4
- encryption 253–71
 - algorithms 255, 257–8
 - awareness training 60
 - backups 218, 253–4
 - data theft 248
 - email 265–7
 - file transfer protocol 100
 - hardware theft 373
 - information security policies 51
 - key exchange problem 268–70
 - key strength 257–8
 - legislation 29
 - off-site computers 303–4
 - passwords 36–9, 113
 - portable devices 260–2
 - prime factors 258–60
 - problems 256–7
 - public key 266, 268–70
 - recovery procedures 267–8
 - risk analysis 13
 - security through obscurity 142–3, 145
 - Windows Vista 150, 151
- Enigmail 266
- enterprise-level backups 219–20
- error messages 182–3, 366
- Ethereal 296, 298
- ethernet sockets 92
- European Institute for Computer Antivirus Research (EICAR) 181–2
- Event Viewer 76
- exchange servers 137–8
- .EXE files 83–4, 157
- expiry dates 320, 323, 325
- facecode.co.uk 42
- fake email 154–6
- false instruments 29
- Fanning, Shawn 203–4
- FAT/FAT32 filing system 71–2, 262–3
- file compression 266
- file extensions 83–4, 352
- file integrity 330
- file sharing 78–82, 188, 203–8, 273
- file transfer protocol (ftp)
 - data interception 296–7
 - encryption 256, 267
 - firewalls 100, 102
 - off-site computers 303–4
 - passwords 38
 - search engines 282
 - security through obscurity 143
 - server security 96
 - Web sites 110
 - workstation security 80
- FileLocator Pro 355
- filenames 352
- filetype keywords 282
- fingerprints 14, 41–4, 348
- firewalls 99–107
 - bypassing 105–6
 - demilitarized zones 104
 - file sharing 207
 - hacking competitions 106–7
 - human 315
 - information security policies 51
 - intrusion detection systems 327

- firewalls (*continued*)
 - logs 21–2, 29, 102–4
 - messenger popups 193–4
 - off-site computers 274, 275–6, 303, 309
 - personal 101
 - port numbers 100–1, 102
 - reporters 103
 - risk analysis 15, 17, 18, 19
 - spyware 190
 - stateful packet inspection 101
 - stealth mode 104
 - Web sites 110
 - webcam security 232
 - Windows Vista 149–50
 - Windows workstation security 72
- floppy disks 176–7, 253
- ForceGuest 78–9
- forensics 345–57
 - covert monitoring 350–1
 - deleted files 354–5
 - hidden evidence 351–3
 - Internet activities 353–6
 - logs 345–7, 352–3, 354
 - metadata 352, 355–6
 - resources 356–7
 - seizing a computer 347–50
 - when to act 347, 356
- Forgery and Counterfeiting Act 2
- form variable tampering 122–3
- FotoSense 117
- fraud 13–14, 20, 118, 158–63, 319–26
- Freedom of Information Act 30
- ftp *see* file transfer protocol
- full system backups 210, 219
- full-face recognition 42
- GetDataBack 220–1
- GFI LANguard Network Security Scanner 137
- Ghost 211, 349
- good viruses 174
- Google 279
- Google Hacking 281–4
- GotoMyPC 305–6
- Guidance Software 349–50, 353
- hacking competitions 106–7
- hacking tools 24–5, 191, 200, 353
 - brute force attacks 114
 - passwords 36
 - penetration testing 134–5, 138
 - port scans 102, 104
 - security through obscurity 142
 - wireless networking 126, 129
- handhelds *see* portable devices
- hard disks 348–9
- hardening Windows 77
- hardware
 - disposal 52
 - installation 73
 - theft 369–73
- Herson, David 257
- heuristics 180–1
- HFNetChk 67, 68
- Hidden Data Removal Tool 239
- hidden evidence 351–3
- hidserv.exe 182
- hoaxes 182–3
- home workers *see* off-site computers; portable devices
- homepage resetting 186
- honeynets 21
- host-based intrusion detection systems 328–9
- hot lists 324–5
- Hotmail 165, 168, 248
- htaccess/htpasswords 112–14, 280
- HTML *see* hypertext markup language
- human firewalls 315
- hypertext markup language (HTML) 156–7, 159

- iana.org 81
- IBM 19
- identity management 292–3
- identity theft 118, 191, 322, 325
- IDS *see* intrusion detection systems
- IFPI *see* International Federation of the Phonographic Industry
- IHCF *see* Industry Hot Card File
- indemnity insurance 133
- index.htm files 282–3
- Industry Hot Card File (IHCF) 324–5
- information security policies 47–53
- Information Security Policies Made Easy* (Wood) 49
- infrared 129
- injection attacks 325
- Inland Revenue Service (IRS) 135
- insider trading 259
- insiders 11, 244–5
 - awareness training 59
 - data interception 296
 - penetration testing 133
 - risk analysis 17–19
 - spam 167–8
- installation files 144
- installation keys 200
- installers 188, 210–11
- insurance 133, 360–1, 371
- integrity, email 265
- integrity checkers 330
- intellectual property (IP) 195, 283–4, 320–1
- intelligence agencies 257, 259, 261, 297
- interception of data 295–9
- internal id numbers 263–4
- International Federation of the Phonographic Industry (IFPI) 207–8
- Internet Explorer 82, 149–50
- internet forums 52
- internet misuse 227–35
 - blogs 232–3
 - cuckoo sites 233–4
 - image investigation 230
 - online banking 234
 - Web filters 229
 - webcam security 231–3
- Internet Relay Chat (IRC) 169
- intrusion detection systems (IDS) 138, 327–32, 334, 336
- intrusion prevention systems (IPS) 330–1
- Investor Protection Act 29
- Iomega 213
- IP *see* intellectual property
- IP addresses 89–90, 100–3, 114, 277, 302–3, 372
- iPods 249, 340
- IPS *see* intrusion prevention systems
- IRC *see* Internet Relay Chat
- iris recognition 41
- Iron Mountain 254
- IRS *see* Inland Revenue Service
- ISO 17799 23, 25–7
- itsecurity.com 4
- iTunes 204–5
- Jaschen, Sven 25
- Javascript 120, 169–70
- Johansen, Jon 260
- Kaspersky Administration Kit 180
- Kazaa 204, 207, 321
- Kensington locks 371
- key exchange problem 268–70, 335
- key generators 200
- key strength 257–8
- keyghost.com 192
- keystroke loggers 21, 190–2
 - data interception 295
 - encryption 259–60
 - forensics 350–1

- keystroke loggers (*continued*)
 - passwords 36, 39, 45–6
 - server security 91–2
 - shared computers 305
 - viruses 175
- L0phtCrack 38–9
- LaCie 42
- LAN *see* local area networks
- LANguard Network Security Scanner 137
- laptops
 - encryption 260–2
 - hardware theft 369–73
 - information security policy 52
 - patch management 66
 - personal 274
 - protecting 370–3
 - viruses 178
 - Windows Vista 148
- legislation 2, 23–5, 27–31
 - backups 216, 221–2
 - denial of service attacks 286
 - encryption 257, 259–60
 - information security policies 51
 - penetration testing 138
 - wireless networking 126–7
- Lexmark 186
- license agreements 197–8, 199–200, 211
- line tapping 295–7
- link files 223–4
- Linux 90–1, 174, 183, 309
- listening ports 80–2
- liutilities.com 186
- Lloyds TSB 160–1
- local area networks (LAN) 78–9
 - firewalls 100, 101, 104, 105–6
 - off-site computers 277, 307
 - viruses 176
 - wireless networking 127–9
- Local Password Policy 33, 46
- Local Security Policies 76–7
- locking down 341
- lockout policy 76–7
- Log Me In 305–6
- logs
 - cuckoo sites 233
 - firewalls 102–4
 - forensics 345–7, 352–3, 354
 - internet misuse 230
 - IP addresses 114
 - Web servers 111
- Lotus 145
- Lynn, Michael 258–9
- MAC *see* media access control
- McAfee 179, 180, 275
- Macintosh 174, 183
- macros 157, 183
- mail servers 95–6
- mailinator.com 169
- MakeMeAdmin 75
- managed security services providers (MSSPs) 333–8
- markup 238–40
- MBSA *see* Baseline Security Analyzer
- media access control (MAC) addresses 128
- MessageLabs 166
- messenger popups 193–4
- META tags 281, 282
- metadata 238–40, 352, 355–6
- method123.com 16
- Micronet 800 8–11
- Microsoft
 - Baseline Security Analyzer 22, 68–9, 137, 179
 - Best Practice Analyzer 137
 - Data Protection Manager 218, 219–20
 - encrypting file system 74, 262–5, 266–7, 303–4

- metadata 239–40
 - Outlook 177
 - patch management 65–9
 - piracy 197–8, 199–200
 - Server Update Services 66–7
 - Small Business Server 90–1
 - spam 165, 167, 170
 - Windows Vista 147–52
- MIME 266
- Mitnick, Kevin 315
- mobile phones 249, 320
- modems 8–9, 36, 105–6, 192–3
- monitoring staff activity 30, 163–4
- most recently used (MRU) files lists 355
- MP3 files 203, 205–7, 240
- MRU *see* most recently used
- MSSPs *see* managed security services providers
- multiple protection methods 143–4
- myirock.com 129
- MySQL databases 110, 114, 118–20
- Napster 203–4
- NAT *see* network address translation
- National Infrastructure Security Coordination Centre 69
- need to know rule 250, 296, 315–17
- Net Intelligence 230
- netsquare.com 96
- netstat command 80–1
- NetStumbler 126, 129, 297–8
- network address translation (NAT) 276–8
- network-based intrusion detection systems 328–9
- networks
 - access protection 150
 - domain-based 4, 72–3
 - protocol analyzers 296–7
 - wireless 20, 125–30, 270, 278
- see also* local area networks; virtual private networks
- nisc.gov.uk 69
- nmap 102
- nmap port scanner 138
- non-repudiation 265–6, 269
- non-routable IP addresses 277
- Norton Ghost 211, 349
- Norton Personal Firewall 275
- NTFS filing system 71–2, 262–3
- obsolescence 217–18, 223
- off-site computers 273–8, 301–10
 - file transfer protocol 303–4
 - firewalls 274, 275–6
 - remote access 305–8
 - shared computers 304–5
 - virtual private networks 270, 307–8
 - viruses 302–3, 305
- offensive material 27–9, 228, 351
- one-time passwords 44–5
- online banking 234
- Open Web Application Security Project (OWASP) 120
- opensourcecms.com 119
- opsi.gov.uk 25, 27
- Out of Office messages 168–9
- Outlook 177
- outsourcing 333–8
- OWASP *see* Open Web Application Security Project
- own-brand encryption 257–8
- P2P *see* peer-to-peer
- padlock symbol 21, 150, 160, 191, 270
- padlock symbol *see* secure sockets layer
- palmtops *see* portable devices
- partial passwords 39
- Pasco 354
- passwords 9–10, 33–46
 - administrators 35
 - authentication 39–41

- passwords (*continued*)
- awareness training 60–1
 - basic HTTP authentication 112–14
 - biometrics 41–4
 - changing 316–17
 - complexity requirements 33–4
 - cracking 36–7
 - data interception 298
 - data theft 250
 - default 35–6
 - dictionary attacks 36–7
 - duress 42–3
 - encryption 36–9, 256, 259–60, 268
 - file transfer protocol 38
 - forensics 351
 - generators 113
 - information security policies 52
 - keystroke loggers 36
 - legislation 2
 - one-time 44–5
 - outsourcing 335, 337
 - partial 39
 - penetration testing 135
 - phishing attacks 159
 - policies 33–5, 39
 - provisioning 289–93
 - recovery software 37–9
 - resetting 34–5
 - risk analysis 14
 - search engines 282
 - server security 91–2
 - shared computers 304
 - social engineering 313, 314–17
 - spyware 187
 - Web sites 110, 112–14
 - Windows workstation security
 - 72–3, 76–7
 - wireless networking 128
- patch management 65–9, 119, 121–2
- pay-as-you-go phones 320
- Papal 123
- PC Anywhere 306
- PC Tools 85, 189
- Pads *see* portable devices
- peer-to-peer (P2P) systems 204
- penetration testing 105, 131–9
- personal email 163–4
- personal firewalls 101
- personal information
 - data theft 247
 - encryption 254, 256, 261
 - search engines 283–4
 - social engineering 313, 316
- PGP *see* Pretty Good Privacy
- pharming 161–2
- phishing attacks 40, 59, 150, 158–61
- phone preaching 159
- PHP scripting language 114, 116
- physical access 91–4, 237, 339–43
- PIN codes 322–6
- piracy 195–201, 207, 260
- Dialer 230
- PKI *see* public key infrastructure
- Pointsec 86, 262
- political hacking 11, 17
- popups 193–4
- pornography 27–9, 228, 351
- port numbers
 - firewalls 100–1, 102
 - security through obscurity 143
 - tunnelling attacks 327
- port scanners 19
 - firewalls 101–2, 104
 - penetration testing 134, 138
 - security through obscurity 143
 - social engineering 313
- port traffic 80–2
- portable devices 260–2, 267, 304
 - see also* laptops; USB devices
- power protection 94–5
- Powergen 115
- premises 339–43

- Prestel 8–11
- Pretty Good Privacy (PGP) 269
- prime factors 258–60
- privacy 30
- Privacy and Electronic Communications (EC Directive) Regulations 28
- private investigators 18
- privilege levels 9, 147–8, 250
- product launches 115
- product reviews 3
- proprietary encryption 257–8
- Protection of Children Act 27–8
- provisioning 289–93
- proximity badges 342
- proxy servers 51, 302–3
- pseudo-photographs 28
- public access 341
- Public Company Accounting Reform 29
- public key encryption 266, 268–70
- public key infrastructure (PKI) 270
- quotas 82–3
- radio waves 297
- RAID *see* redundant array of independent disks
- random hacking 11, 17
- recovery agents 264
- recovery procedures 267–8
- recovery software 37–9
- redundant array of independent disks (RAID) 96–7
- redundant hardware 85–6
- registration keys 200
- registry 84–5, 148–9, 210
- Regulation of Investigatory Powers Act 27
- remote access 175, 305–8
- remote desktop 306–7
- resetting passwords 34–5
- rich text format (RTF) 156–7
- ripe.net 103
- The Risk Advisory Group (TRAG) 245
- risk analysis 13–22, 246–9
 - complacency 16–17
 - honeynets 21
 - identifying risks 14–15
 - insiders 17–19
 - risk registers 16
 - statistics 19–20
- risk registers 16
- robots 174–5, 286–7
- robots.txt files 280
- rogue diallers 192–3
- role-based provisioning 291
- rollback facilities 67–8
- routers 276
- RTF *see* rich text format
- Run As option 75
- S/MIME 266
- Sasser virus 25
- SBS *see* Small Business Server
- .SCR files 84
- scrambling 265
- screen grabbers 176, 190–2
- Sealed Media 198–9
- search engines 182–3, 187
 - error messages 366
 - hacking techniques 279–84
 - prohibiting 280–1
 - security through obscurity 142
- secure sockets layer (SSL) 21, 150, 160, 191, 270
- secure startup 151
- securesite.com 304
- SecurID authenticator 40–1
- Security Assessment Tool 69
- security awareness training 18, 26, 55–63

- security through obscurity (STO)
 - 141–6
- security-survey.gov.uk 19–20
- securityguidance.com 69
- seizing a computer 347–50
- Sender ID 170
- Sender Policy Framework (SPF) 170
- serial numbers 200, 372
- server security 89–98
 - administrator passwords 91–2
 - physical security 91–4
 - power protection 94–5
 - RAID 96–7
 - welcome banners 95–6
- Server Update Services (SUS) 66–7
- service level agreements (SLAs) 336
- service set identifier (SSID)
 - broadcasting 127
- Sex Offences Act 28
- shared computers 304–5
- Shavlik 67–8
- sheep dip computers 274
- shortcuts 223–4
- shoulder-surfing 39, 45–6
- shredders 93
- signature databases 180–1
- SiSoft Sandra 106
- SLAs *see* service level agreements
- slowdown 186
- Small Business Server (SBS) 90–1
- smart cards 40, 151
- Smart Water 372
- smoke-based theft deterrents 372
- SMTP servers 154–6
- social engineering 311–17
 - data theft 247
 - firewalls 107
 - need to know rule 315–17
 - penetration testing 135
 - physical entry 340
 - search engines 283–4
- software crackers 145
- software installation 50, 73
- Solomon, Alan 214
- Sophos 232
- sound analyzers 297
- source code 247, 321, 325
- spam 116, 165–72
 - awareness training 59
 - detection 166–8
 - prevention 168–70
 - replying 168, 171–2
 - spoofed email 154–6
 - viruses 174
- Spam Assassin 166–7
- SPF *see* Sender Policy Framework
- SPI *see* stateful packet inspection
- spidering 280
- Spinrite 220–1
- spoofed email 154–6
- Spybot Search and Destroy 189–90
- spying 245, 257
- spyware 157, 185–90, 274
- SQL injection 120–2
- SSID *see* service set identifier
- SSL *see* secure sockets layer
- standards 23, 25–7, 245, 255, 257–8, 365
- stateful packet inspection (SPI) 101
- stealth mode 104
- steganography 352
- STO *see* security through obscurity
- Stonylake Firewall Reporter 103
- stumbler.net 129
- Sunbelt Software 137, 189
- surfing *see* internet misuse
- surveillance 51, 191
- SUS *see* Server Update Services
- Symantec 38, 72, 165–6, 182, 211, 349
- System Restore 181
- systems failure 19, 20

- tabloid journalism 18, 245
- task manager 185–6, 191, 193
- TCP/IP 82, 100, 102
- telecommunications legislation 28
- telephone verification 325
- telnet 154–6, 296–7
- Tempest 297
- temporary admin permissions 74–5
- terrorism 111, 206, 214, 216
- text editors 238–9
- Thawte 270
- The Risk Advisory Group (TRAG) 245
- theft 20
 - ATM machines 311–12
 - data 243–51
 - hardware 369–73
 - identity theft 118, 191, 322, 325
- thesaurus functionality 167
- Thor Technologies 290
- three-finger salute 75–6
- Tiger Teams 132
- Todd, Mike 166
- TPM *see* trusted platform module
- track changes facility 238–9
- TRAG *see* The Risk Advisory Group
- Trojan Horses
 - denial of service attacks 286–7
 - encryption 259–60
 - firewalls 101, 102
 - internet misuse 232, 234
 - malware 188
 - passwords 39
 - server security 91–2
 - viruses 173
- TrueActive 191, 350–1
- trusted platform module (TPM) chips 151
- Tsunami site case 138
- tunnelling attacks 100–1, 327
- two-dimensional provisioning 291–2
- UDO *see* Ultra Density Optical
- Ultra Density Optical (UDO) 223
- unauthorized access 20, 24
- uninterruptible power supplies (UPS) 94–5
- UNIX 199, 309
- UPS *see* uninterruptible power supplies
- USB devices
 - data theft 248–9, 253
 - encryption 263, 267
 - forensics 352
 - internet misuse 231
 - passwords 42
 - premises security 340
 - server security 92
- user accounts 72–5, 78–9, 148, 149
- usernames 9–10, 36–7
 - basic HTTP authentication 112–13
 - encryption 263–4
 - shared computers 304
 - social engineering 314–15
- velocity of change 325
- velocity of use 325
- Verisign 270
- Virgin Atlantic 255–6
- virtual folders 223–4
- virtual private networks (VPNs) 270, 307–8
- viruses 173–84
 - administrator accounts 148
 - attachments 157–8
 - avoiding infection 177–81
 - awareness training 58–60
 - denial of service attacks 286–7
 - file extensions 84
 - firewalls 101
 - functions 174–6
 - hoaxes 182–3
 - HTML email 157

- viruses (*continued*)
 - information security policies 50
 - legislation 24, 25
 - off-site computers 302–3, 305
 - patch management 65–6
 - platforms 174, 183
 - risk analysis 15, 18, 20
 - spoofed email 156
 - spreading methods 176–7
 - System Restore 181
 - testing antivirus software 181–2
 - USB devices 249
 - Windows workstation security 72
 - see also* antivirus software
- visitors 178–9, 341
- Vista (Windows) 147–52
- VNC 306
- Vogon 221
- Voice over IP (VoIP) 171
- VoIP *see* Voice over IP
- VPNs *see* virtual private networks
- vulnerability scanning 137–8

- WAP *see* wireless access points
- WAV files 203
- Web filters 229
- Web Historian 354
- Web proxy servers 51
- Web servers 80, 199
 - encryption 256
 - firewalls 99–100, 101, 104
 - logs 111
 - Web sites 109
- Web sites 109–24
 - backing up 110–11, 120
 - basic HTTP authentication 112–14
 - brute force attacks 114
 - checksum programs 111
 - database-driven 110, 114, 116–20
 - defacement 110–11
 - domain names 114–16
 - hacking techniques 120–3
 - patch management 119, 121–2
 - updating 117
- Web surfing 50, 60
- webcam security 231–3
- Webmin 309
- WebSense 229
- welcome banners 95–6
- WEP *see* wired equivalent privacy
- WiFi *see* wireless networking
- WiFi sniffing 295–6, 297–8
- Windows Vista 147–52
- Windows workstation security
 - 71–87
 - BIOS pages 77
 - default accounts 78–9
 - disk quotas 82–3
 - file extensions 83–4
 - file sharing 78–82
 - formatting hard disks 71–2
 - Internet Explorer 82
 - netstat command 80–1
 - port traffic 80–2
 - redundant hardware 85–6
 - registry 84–5
 - temporary admin permissions 74–5
 - three-finger salute 75–6
 - user accounts 72–5, 78–9
 - winternals.com 91–2
 - winwhatwhere.com 350–1
 - wired equivalent privacy (WEP) 127, 128
 - wireless access points (WAP) 92, 125, 278
 - wireless local area networks (WLAN) 127–9, 307
 - wireless networking (WiFi) 20, 125–30, 135–6, 278

- wireless protected access (WPA) 127, 128
- WLAN *see* wireless local area networks
- Wood, Charles Cresson 49
- WPA *see* wireless protected access
- ws-ftp.ini file 282
- zip files 157, 266
- zombie robots 174–5, 286–7
- ZoneAlarm 72, 275
- Zotob virus 65–6
- Ztree 355