## INDEX

## A

abuse, detecting, 77 access policies, 124 clean-desk policies, 124-125 closed-blind policies, 124 departing employees, 123 job categories, 123 password sanctity, 124 access attacks, 15 access strategems, 16 data-driven attacks, 37 impersonation attacks, 36 man-in-the-middle attacks, 38 password attacks, 36 protocol exploitation, 37 session hijackings, 37 session replay, 38 social engineering, 36 software exploitation, 37 Trojan horses, 37 trust exploitation, 37 viruses. 37 worms, 37 access cards, 68-69 access control lists, routers, 107 access control servers (ACSs), 71, 106-107 access integrity, vunerabilities, 8 access points, wireless networks, 264 access warnings, routers, 259-260

access-control policies, 250-252 three-strike access rules, 25 accounting, 66, 71-72 ACSs (access control servers), 71 ALE (annual-loss expectancy), 223-224 analog Internet access policies, 253 authentication, 255 dialup workstations, 254 fax line use, 254 inbound dialing, 255 one-time passwords, 254 outgoing traffic monitoring, 254 password storing, 255 war dialers, 253-254 annualized rate of occurrence (ARO), 223 annual-loss expectancy (ALE), 223-224 APM, 107-108 **APM** (automated patch management), 98-100, 107-108 application layer attacks, threat mitigation technologies, 108 applications as invasion targets, 45 design issues, vunerabilities, 5 encryption, 60 ArcSight, 93-94 ARO (annualized rate of occurrence), 223

assessment tools, 89-90 penetrable analysis, 90-92 ticket assignments, 92 vunerability scans, 90 assets protection, choosing, 203 value estimations, SLE (single-loss expectancy), 221 attack threads, 28-29 attacks, 22 abuse, detecting, 77 access attacks, 15 access strategems, 16 data-driven attacks, 37 impersonation attacks, 36 man-in-the-middle attacks, 38 password attacks, 36 protocol exploitation, 37 protocol vunerabilities, 15 session hijackings, 37 session replay, 38 social engineering, 36 software exploitation, 37 Trojan horses, 37 trust exploitation, 37 viruses, 37 worms, 37 application layer attacks, threat mitigation technologies, 108 brute-force attacks, 25 calssifying, IDSs (intrusiondetection systems), 77 categories, 9-21 characteristics, 36-40 costs ALE (annual-loss expectancy), 223–224 alternatives, 220-224 ARO (annualized rate of occurence), 223 baseline determination. 218-220 examining, 218 SLE (single-loss expectancy), 220-223

detection, IDSs (intrusiondetection systems), 76-78 DoS (denial of service) attacks, 16-17, 104-106 bandwidth consumption, 17-19 buffer overflow, 17-19 DDoS (distributed denial of service) attacks, 19-21 detecting, 77 domain name hijackings, 19 mail bombs, 18–19 threat mitigation technologies, 106 exploitation attacks, detecting, 77 human nature, 10-11 impersonation, 25 IP spoofing, threat mitigation technologies, 107 long-term risks, 203 man-in-the-middle attacks, threat mitigation technologies, 107 network reconnaissance, threat mitigation technologies, 107 packet sniffers, threat mitigation technologies, 107 password attacks, 25 threat mitigation technologies, 107 port redirection attacks, threat mitigation technologies, 108 preventing, IPSs (intrusionprevention systems), 81 protocol exploitation, 27 RA (risk aversion) quotient, 204 calculating, 205 risk tolerance equivalency scale, 206 reconnaissance attacks, 11–14 detecting, 76 eavesdropping, 23–25, 36 footprinting, 22–23, 36 scanning and system detailing, 23-24, 36 topology mapping, 15

#### bugs

reporting, IDSs (intrusiondetection systems), 77-78 risk aversion, 200-201 risk exposure, lowering, 105-108 risk tolerance, determining, 202-203 sabotage attacks, 104 short-term risks, 203-204 social engineering, 33-35 software exploitation, 27 system penetration attacks, 104 targets, 104-105 threads, 28-29 trends, 104-105 Trojan horses, 28 threat mitigation technologies, 108 trust exploitation attacks, 26 threat mitigation technologies, 108 unauthorized access attacks, 104 threat mitigation technologies, 107 viruses, 28, 104 threat mitigation technologies, 108 war-dialers, threat mitigation technologies, 106 wireless intrusions, 30, 38-39 DoS (denial of service) attacks. 32 drive-by spamming, 32 eavesdropping, 30-31 frequency jamming, 33 man-in-the-middle attacks, 31 walk-by hacking, 32 worms, 27-28 threat mitigation technologies, 108 audit tools, 89, 92 correlation tools, 93–94 forensic analysis, 94–95 honeypots, 96 log analysis, 94-95 normalization, 93

auditing, 122 Cisco security wheel, 287 authentication, 66-67 access cards, 68-69 Cisco security wheel, 282 encrypted VPN, 62 passwords, 67-68 OTPs (one-time passwords), 67-68 tokens. 68 policies, 255 strong authentication, 68-70 PINs (personal identification numbers), 70 static biometrics, 70 tokens. 69-71 authorization, 66 software, 248 authorization servers, 71 automated patch management (APM), 98-100 AV (antivirus) software, 48-50 AV engines, 49 multiple brands, utilizing, 50 AV engines, 49 availability, equipment, managing, 125-126 awareness levels, threats, 4

## В

backup data handling, 249
bandwidth consumption, 16

DoS (denial of service) attacks, 17–19

baselines, attack costs

alternatives, 220–224
determining, 218–220

basic network topology (SAFE), 113
bio-tokens, 71
brute-force attacks, 25
buffer overflow, DoS (denial of service) attacks, 17–19
bugs, 45

business continuity planning, 137–138 business relationships, building, 157–158

# С

CA (certificate authority), 72 calculating RA (risk aversion) quotient, 205 **CCNP Self-Study Building Scalable Cisco** Internetworks (BSCI) (I), 2nd Edition. 309 **Centre for Safe and Responsible** Internet Use (CSRIU), 296 Certificates, CA (certificate authority), 72 change control, 127 **Cisco NAC (network admission** control), 97 Cisco SA (Security Agent), 96 **Cisco SAFE Blueprint, 40, 308** application targets, 45 host targets, 43 network targets, 43-45 router targets, 41 switch targets, 41–42 Cisco security wheel, 280-281 improve component, 287-288 change implementations, 289 policy adjustments, 288 monitor component, 284-285 data collection, 285 IDSs (intrusion-detection systems), 285 **IPSs** (intrusion-prevention systems), 285 network vunerability scanners, 287 retention, 285 secure component, 281-282 authentication, 282 encryption, 283

firewalls, 283 vunerability patching, 283-284 test component, 286 auditing, 287 responsibility determination, 286 classifications, attacks, IDSs (intrusion-detection systems, 77–78 clean-desk policies, 124-125 closed-blind policies, 124 combo-malware, 28 communications, peer groups, vunerabilities, 9 compliance, policies, 134-136 corporate compliance, 134 user compliance, 135-136 comprehensive backup data handling, 249 comprehensive network topology (SAFE), 116-117 **Computer Crime and Security** Survey 2003, 308 Computer Security Handbook, 4th Edition, 308 confidentiality, encrypted VPNs, 62 confidentiality levels, determining, 128-129 contactless cards, 69 content filtering, 83 e-mail content filtering, 88-89 URL filtering, 83-84 outgoing-traffic administration. 85-87 tools, 84-85 continuity planning, 137-138 CoOP (continuity, or continuity of operations), 242 corporate compliance, policies, 134 corporate organizations, engagement methods, 175-188 correlation tools, 93-94 costs, attacks ALE (annual-loss expectancy), 223-224

alternatives, 220-224 ARO (annualized rate of occurrence), 223 baseline determination, 218-220 examining, 218 SLE (single-loss expectancy), 220-223 **CSI/FBI** Computer Crime and Security Survey 2004, 308 CSRIU (Centre for Safe and **Responsible Internet Use)**, 296 cultures secure cultures, 173 creating, 130–132 security, instilling, 158-159 custom-written software, policies, 126-127

## D

data collection, Cisco security wheel monitor, 285 data sensitivity policies, 268–272 data transfers, privacy concerns, 128 data-driven attacks, 37 DDoS (distributed denial of service) attacks, 16, 19-21 decentralized policy enforcement, 155 deliverables, acknowledging, 171-173 demilitarized-zone (DMZ) web server. See DMZ (demilitarized zone) web servers departing employees, policies, 123 departments, security incidents, effects on, 190 design issues, vulnerabilities, 5-6 devices availability, managing, 125–126 budgeting for, 224 present values, 227-230 TCO (total cost of ownership), 225–227

hardening devices, vunerabilities, 7 unsecured devices, vunerabilities, 6 dialup Internet access, policies, 253 authentication, 255 dialup workstations, 254 fax line use. 254 inbound dialing, 255 one-time passwords, 254 outgoing traffic monitoring, 254 password storing, 255 war dialers, 253-254 dialup workstations, policies, 254 digital certificates, 72 digital signatures, 74 diminishing returns, security modeling, 213-214 directives, understanding, 170-171 discount factor, equipment, 229 DMZ (demilitarized-zone) web servers firewalls, 57-58 network policies, 260-261 doing just enough state, 174 doing too much state, 174 domain name hijackings, 19 Don't Panic. Plan, 308 DoS (denial of service) attacks, 16-17, 104-106 bandwidth consumption, 17-19 buffer overflow, 17-19 DDoS (distributed denial of service) attacks, 19-21 detecting, 77 domain name hijackings, 19 mail bombs, 18-19 threat mitigation technologies, 106 wireless intrusions, 32, 39 drive-by spamming, 39 wireless intrusions, 32

# Ε

Eavesdropping attacks, 23-25, 36 wireless intrusions, 30-31, 38 e-mail, content, filtering, 88–89 employee sabotage, legislation regarding, 291-292 employees business relationships, building, 157 - 158secure cultures, involving in, 130-131 encrypted VPNs, 60-63 authentication, 62 confidnetiality, 62 hashing, 62 integrity, 62 remote user, 61 secure data exchanges, 62 site-to-site, 61 VPN concentrators, 63 encryption, 59-60 applications, 60 CA (certificate authority), 72 Cisco security wheel, 283 digital signatures, 74 encrypted VPNs, 60-63 authentication, 62 confidentiality, 62 hashing, 62 integrity, 62 remote user, 61 secure date exchanges, 62 site-to-site, 61 VPN concentrators, 63 encryption keys, 59 lifetimes, 60 file encryption, 65-66 keys, distribution, 72 mobile employees, 248 policies, 128 expectation levels, 258–259 session time length, 257 standards, 258

SSL (Secure Sockets Layer) encryption, 63-65 environments secure environments, 173 creating, 130-132 establishing, 156–157 instilling, 158-159 equipment availability, managing, 125-126 budgeting for, 224 present values, 227-230 TCO (total cost of ownership), 225-227 equipment paths, 161 ethics policies, 268-272 executive involvement, IT security, 162 - 165exploitation attacks, detecting, 77 exposure factor, SLE (single-loss expectancy), 222 extranets, network policies, 262-263 extrapolating policy intent, vunerabilities, 8

# F

false positives, IPS sensors, correcting, 82 fax lines, dialup and analog policies, 254 file encryption, 65-66 filtering content filtering, 83 e-mail content filtering, 88-89 URL filtering, 83–87 MAC addresses, 54 traffic filtering, 50-51 advanced filtering, 55-58 basic filtering, 51–54 equipment, 59 filters, privacy filters, notebook computers, 100-101

finance department, security incidents, effects on, 190 financial modeling, 218 Financial Modernization Act of 1999, 294 FirewallAnalyzer, 94 firewalling, stateful firewalling, 55-58 firewalls, 58, 107-108 Cisco security wheel, 283 DMZ (demilitarized-zone) web servers, 57-58 interdepartmental firewalls, 56-57 network policies, 260 standby firewalls, 116 footprinting, 22-23, 36 forensic analysis, audit tools, 95 forensic analysis tools, 94 frequency jamming, 39 wireless intrusions. 33

# G-H

GNU-PGP, 65 governance, security, 152–153 Gramm-Leach-Bliley Act, 294 guidelines, creating, procedural requirements, 132-134 hacking legislation regarding, 291 sniffing, 25 walk-by hacking, 32 Hacking Exposed: Network Security Secrets & Solutions, 4th edition, 309 hardening devices, vunerabilities, 7 hardware, 48 installation, policies, 248 traffic filtering, 59 hashing digital signatures, 74 encrypted VPN, 62 header-modified requests, 20 Health Insurance Portability and Accountability Act (HIPAA), 294 HIDS (host-based IDS), 78–79, 106-108 homeland, securing, 159 equipment paths, 161 incident reporting, 159–161 vunerable point acknowledgements, 161–162 honeypots, 96 host-based IDS (HIDS), 78–79 hosts as invasion targets, 43 human issues, vulnerabilities, 6-7

**IDSs**, 75 attacks classifying, 77–78 detection, 76-77 reporting, 77-78 HIDS (host-based IDS), 78-79 management server consoles, 78 NIDS (network-based IDS), 78-79 target-based IDSs, 82-83 IDSs (intrusion-detection systems), Cisco security wheel monitor, 285 IM (Infosec management) quotient surveys, 148-149, 168 analyzing, 206 conducting, 144-148 generating, 204-206 imperatives, acknowledging, 171-173 impersonation attacks, 25, 36 implementation issues policies, 246-247 vulnerabilities, 7 access integrity, 8 extrapolating policy intent, 8 password policies, 8 peer group communications, 9 policy enforcement challenges, 9

improve component, Cisco security wheel, 287-288 in-band management, 42 inbound dialing, policies, 255 incident reporting, 159-161 Information Security, 309 **Information Security Breaches** Survey 2002, Technical Report, 309 **Information Security Breaches** Survey 2004, Executive Summary, 309 **Information Security Breaches** Survey 2004, Technical Report, 309 Infosec management (IM) quotient surveys, 148-149, 160 analyzing, 206 conducting, 144-148 generating, 204-206 Infosec operational (IO) quotient surveys, 168 analyzing, 206 generating, 205-206 initiatives, directing, 153 decentralized policy enforcement, 155 steering committees, 154-155 integrity, encrypted VPN, 62 integrity issues, legal ramifications, 294-295 interactivity, regulating, 128 confidentiality levels, 128-129 inventory control, 129–130 interdepartmental firewalls, 56-57 Internet access control, 248 **Internet Requests for Comments** (RFCs), 309 intitiatives (security), 153 intrusion-detection systems (IDSs). See IDSs (intrusion detection systems) inventory control, implementing, 129-130

investments (security), 152 financial modeling, 218 governance, 152-153 returns, analyzing, 230-236 ROI (return on investment) modeling, 152 ROP (return on prevention), 4, 152 investor relations department, security incidents, effects on, 190 IO (Infosec operational) quotient surveys, 168 analyzing, 206 figuring, 194 generating, 205-206 questions and situations, 191-194 rating scale, 191 respondents, delivering to, 190-191 senior management requirements, assessing, 188-194 IP spoofing, threat mitigation technologies, 107 **IPSec**, 107 The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 308 **IPSs** (intrusion-prevention systems), 75, 79-82 attacks, shunning, 81 Cisco security wheel monitor, 285 packets, 80 sensors, training, 82 session termination, 81 IRR (internal rate of return). 233 - 234ISDs (intrusion-detection systems), 75 **IT** management corporates mandates understanding, 170-171 deliverables acknowledging, 171–173 imperatives acknowledging, 171–173

organizations engagement methods, 175–188 ROP corporate goals, 169–175 ROP (return on prevention) discussing, 168–169 surveying, 143–144 IM (Infosec Management) quotient, 148–149 IM (Infosec Management) survey, 144–148 IT security, 162 evolution of, 152 executive involvement, 162–165

# J-K

job categories, policies, 123 jurisprudence, 290 employee sabotage, 291–292 hacking, 291 integrity issues, 294–295 negligence, 292–293 netizenry, 295–296 privacy breaches, 293–294

#### keys

distribution, 72 encryption keys, 59 *lifetimes, 60* PKI (public key infrastructure), 72-74 private keys, 73 public keys, 73 **Kirkpatrick, David, 309** 

laptop computers, privacy filters, 100–101 law of diminishing returns, security modeling, 213–214 legislations, 290 employee sabotage, 291–292 hacking, 291 integrity issues, 294–295 negligence, 292–293 netizenry, 295–296 privacy breaches, 293–294 licensing, software, 248 lifetimes, encryption keys, 60 lobbying support, IT management, 176–188 log analysis, audit tools, 94–95 logging, inventory control, 129–130 logistics department, security incidents, effects on, 190

# Μ

MAC addresses, filtering, 54 mail bombs, 18-19 management server consoles (IDS), 78 managers, secure cultures, involving in, 131–132 mandates, understanding, 170-171 man-in-the-middle attacks, 38 threat mitigation technologies, 107 wireless intrusions, 31, 38 marketing department, security incidents, effects on, 190 mitigation (threat mitigation), 96 APM (automated patch management), 98-100 application layer attacks, 108 DoS attacks, 106 IP spoofing, 107 man-in-the middle attacks, 107 NBAR (Network-Based Application Recognition), 97 network reconnaissance attacks, 107 packet sniffers, 107 password attacks, 107 port redirection attacks, 108 self-defending networks, 96-97 technologies, 106 Trojan horses, 108 trust exploitation attacks, 108 unauthorized access attacks, 107

viruses, 108 war-dialers, 106 worms, 108 mobile access dialup and analog policies, 253 authentication, 255 dialup workstations, 254 fax line use, 254 inbound dialing, 255 one-time passwords, 254 outgoing traffic monitoring, 254 password storing, 255 war dialers, 253-254 mobile employees encryption, 248 policies, dialup and analog, 253-255 remote-access policies, 255-256 remote configuration policies, 256 VPN policies, 257 modest network topology (SAFE), 114-115 monitor, Cisco security wheel, 284-285 data collection, 285 IDSs (intrusion-detection systems), 285 IPSs (intrusion-prevention systems), 285 network vunerability scanners, 287 retention, 285 monitoring policies, 247-249 Mydoom worm, 100

# Ν

NAC (network admission control), 97 National Cyber Security Partnership (NCSP), 165 NBAR (Network-Based Application Recognition), 97-98 NCSP (National Cyber Security Partnership), 165 negligence, legal ramifications, 292-293 NetForensics, 93–94 NetIQ, 94 netizenry, 295-296 **Network Intelligence**, 93 network interface cards (NICs), 54 network policies, 259 DMZ servers, 260-261 extranets, 262-263 firewalls, 260 routers, 259 access warnings, 259-260 traffic efficacy, 260 servers, 266-268 wireless policies, 263-265 access points, 264 World Wide Web, 263 network reconnaissance attacks, threat mitigation technologies, 107 network testing, Ciscosecurity wheel, 286 auditing, 287 responsibility determination, 286 network vunerability scanners, Cisco security wheel monitor, 287 **Network-Based Application** Recognition (NBAR), 97-98 network-based IDS (NIDS), 78-79 Newton's Telecom Dictionary: The Official Dictionary of **Telecommunications** Networking and Internet, 16<sup>th</sup> edition, 309 NICs (network interface cards), 54 NIDS (network-based IDS), 78-79 sensors, 106-107 Niksun, 95 No Time to Relax, 309 nonmathematical security fundamentals, 237 normalization, audit tools, 93 **Norton Antivirus Protection** software, 48

notebook computers, privacy filters, 100–101 NPV (net present value), 230–233

# 0

one-time passwords, policies, dialup and analog policies, 254 one-time passwords (OTPs), 67 online banking, SSL (Secure Sockets Layer) encryption, 64-65 operating systems design issues, vunerabilities, 5 policies. 273 operation integrity, managaing, 125-126 opportunities, determining, steering committee, 299-301 OTPs (one-time passwords), policies, 254 outgoing traffic monitoring, dialup and analog policies, 254 outgoing-traffic administration, URL filtering, 85-87 out-of-band management, 42 ownership policies, 133-134

#### Ρ

packet sniffers, threat mitigation technologies, 107 packets, 80 password attacks passwords, 69 attacks, 25, 36 threat mitigation technologies, 107 authentication, 67-68 creating, 251 OTPs (one-time passwords), 67-68 policies password sanctity, 124 vunerabilities. 8 sanctity, maintaining, 248 storing, policies, 255

strong passwords characteristics, 251 incorrect use, 252 tokens. 68 weak passwords, characteristics, 251 patches, APM (automated patch management), 98-100 paths, equipment paths, 161 payback periods, 235-236 peer groups, communications, vunerabilities, 9 penetrable analysis, assessment tools, 90 - 92perimeter routers, traffic filtering, 52 PGP (Pretty Good Privacy), 65 physical security policies, 249-250 Ping of Death attacks, 17 PINs (personal identification numbers), 69-70 PKI (public key infrastructure), 72-74 digital certificates, 72 digital signatures, 74 policies, 242 access, 124 clean-desk policies, 124–125 closed-blind policies, 124 access-control policies, 250-252 adjusting, Cisco security wheel, 288 availability, 125-126 business continuity planning, 137-138 Cisco security wheel, 280-281 improve component, 287-289 monitor component, 284-287 secure component, 281-284 test component, 286-287 compliance, 134-136 corporate compliance, 134 user compliance, 135–136 components, 133 creating, 243-244 criteria, 122

data sensitivity policies, 268-272 decentralized policy enforcement, 155 defining, 134-136 departing employees, 123 determining, 134-136 dialup and analog policies, 253 authentication, 255 dialup workstations, 254 fax line use, 254 inbound dialing, 255 one-time passwords, 254 outgoing traffic monitoring, 254password storing, 255 war dialers, 253–254 efficiency, striving for, 142-143 encryption concerns, 128 encryption policies expectation levels, 258-259 session time length, 257 standards. 258 enforcement, vunerabilities, 9 ethics policies, 268-272 extrapolating policy intent, vunerabilities, 8 formulating, 242 implementing, 246-247 importance of, 122 incidents, handling, 277-278 interactivity, 128 confidentiality levels, 128-129 inventory control, 129–130 IT management, surveying, 143-149 job categories, 123 managing, 138-143 monitoring, 247-249 network policies, 259 DMZ servers, 260–261 extranets, 262-263 firewalls, 260 routers, 259-260 servers, 266-268

wireless policies, 263-265 World Wide Web, 263 operation integrity, 125-126 ownership policies, 133-134 passwords sanctity, 124 vunerabilities. 8 physical security policies, 249-250 privacy concerns, 128 procedural requirements, creating, 132-134 remote-access policies, 255-256 remote configuration policies, 256required policies, determining, 243 retention policies, 268-272 reviewing, 140-141 senior management requirements, assessing, 188-194 software, 126-127 software policies, 273 operating systems, 273 user software, 274-276 virus protection, 273–274 tools, 245-246 types, 277 upholding, 138-143 VPNs, 257 workflow considerations, 142 port redirection attacks, threat mitigation technologies, 108 port security, traffic filtering, 54 present values equipment, 227-230 NPV (net present value), 230-233 presentations, security presentations, 184-186 Pretty Good Privacy (PGP), 65 privacy breaches, legal ramifications, 293-294 confidentiality levels determining, 128-129 policies, 128 Pretty Good Privacy (PGP), 65

privacy filters, notebook computers, 100-101 private keys, 73 private virtual LANs (PVLANs). See **PVLANs (private virtual LANs)** procedural requirements, creating, 132 - 134production department, security incidents, effects on, 190 propagation, worms, 99–100 proposals (security), 152–153 protocol exploitation, 37 protocols design issues, vunerabilities, 6 exploitation, 27 vulnerabilities, hacking into, 15 proximity cards, 69 proxy servers, traffic filtering, 55 pseudo-tokens, 71 **Public Company Accounting Reform** and Investor Protection Act of 2002, The, 295 public key infrastructure (PKI). See **PKI** (public key infrastructure) public keys, 73 PVLANs (private virtual LANs), 53

# Q-R

questions, IO (Infosec Operational) survey, 191–194
RA (risk aversion) quotient, 204 calculating, 205 risk tolerance equivalency scale, 206
rating scale

IO (Infosec Operational) survey, 191

reconnaissance attacks, 11–14 eavesdropping, 23–25, 36 footprinting, 22–23, 36 scanning and system attacks, 23–24

detailing, 36 topology mapping, 15 remote access, VPN policies, 257 remote configuration policies, 256 SSH (secure shell), 256 SSL (secure sockets layer), 256 remote user encrypted VPN, 61 remote-access policies, 255-256 reporting attacks, IDSs (intrusion-detection systems, 77-78 incident reporting, 159-161 **Request for Comments (RFCs), 106** required policies, determining, 243 retention, Cisco security wheel monitor, 285 retention policies, 268–272 return on investment (ROI) modeling, 152, 234-235 return on prevention (ROP). See ROP (return on prevention) returns IRR (internal rate of return), 233 - 234payback periods, 235-236 ROI (return on investment), 152, 234-235 ROP (return on prevention), 4, 152 **RFCs** (Request for Comments), 106 Ridge, Tom, 153 risk aversion, 200-201 RA (risk aversion) quotient, 204 calculating, 205 risk tolerance equivalency scale, 206 risk tolerance, 201-202 determining, 202-203 risk tolerance equivalency scale, 206 risks exposure, lowering, 105-108 long-term risks, 203 short-term risks, 203-204 roconnaissance attacks, detecting, 76

#### **ROI** (return on investment) modeling, 152, 234-235 ROP (return on prevention), 4, 152, 168 analyzing, 230 corporate goals, recognizing, 169-175 discussing with management, 168-169 IRR (internal rate of return). 233 - 234mandates and directives, understanding, 170-171 NPV (net present value), 230-233 payback periods, 235-236 ROI (return on investment), 234-235 routers, 106-107 access control lists, 107 as invasion targets, 41 network policies, 259 access warnings, 259-260 traffic efficacy, 260 perimeter routers, 52 traffic filtering, basic traffic filtering, 51-53 RST (Reset) packets, 80

# S

SA (Security Agent), 96
sabotage attacks, 104
SAFE, 113

A Security Blueprint for Enterprise Networks (SAFE Enterprise), 109–112
basic network topology, 113
comprehensive network topology, 116–117
Extending the Security Blueprint to Small, Midsize, and Remote-User Networks (SAFE SMR), 109, 112–113

IDS Deployment, Tuning, and Logging in Depth (SAFE IDS), 110 IP Telephony Security in Depth (SAFE IP Telephony), 110 modest network topology, 114-115 VPN IPSec Virtual Private Networks in Depth (SAFE VPN). 109 Wireless LAN Security in Depth (SAFE Wireless), 109 Worm Mitigation (SAFE Worm), 110 SAFE architectures, 110–113 SAFE blueprints, 40, 109-110 application targets, 45 host targets, 43 network targets, 43-45 router targets, 41 switch targets, 41–42 sales department, security incidents, effects on, 190 Sarbanes-Oxley Act of 2002, The, 295 Scalability, security postures, 289-290 scanning antivirus software, 49 vunerability scans, assessment tools, 90 scanning and system detailing attacks, 23-24, 36 securecultures, establishing, 156–157 secure environments, 173 security advances in, 48 as learned behavior, 139-140 security audits, 122 security breaches, 22 access attacks, 15 access strategems, 16 data-driven attacks, 37 impersonation attacks, 36 man-in-the-middle attacks. 38 password attacks, 36

protocol exploitation, 37 protocol vunerabilities, 15 session hijackings, 37 session replay, 38 social engineering, 36 software exploitation, 37 Trojan horses, 37 trust exploitation, 37 viruses, 37 worms, 37 brute-force attacks, 25 categories, 9-21 characteristics, 36-40 costs ALE (annual-loss expectancy), 223-224 alternatives, 220–224 ARO (annualized rate of occurence), 223 baseline determination, 218-220 examining, 218 SLE (single-loss expectancy), 220-223 DoS (denial of service) attacks, 16 - 17bandwidth consumption, 17-19 buffer overflow, 17-19 DDoS (distributed denial of service) attacks. 19–21 domain name hijackings, 19 mail bombs, 18-19 human nature, 10-11 impersonation, 25 password attacks, 25 protocol exploitation, 27 reconnaissance attacks, 11–14 eavesdropping, 23-25, 36 footprinting, 22-23, 36 scanning and system detailing, 23-24, 36 topology mapping, 15 social engineering, 33–35 software exploitation, 27

threads, 28-29 Trojan horses, 28 trust exploitation, 26 viruses. 28 wireless intrusions, 30, 38-39 DoS (denial of service) attacks. 32 drive-by spamming, 32 eavesdropping, 30-31 frequency jamming, 33 man-in-the-middle attacks, 31 walk-by hacking, 32 worms, 27-28 security initiatives, directing, 153 decentralized policy enforcement, 155 steering committees, 154-155 security modeling, 207-210 law of diminishing returns, 213-214 requirements, managing, 211-213 topology standards, 207-209 security postures, 289 security presentations, 184–186 SecuritySurvey,DisciplinedSecurity, 308 security topologies, 108-109 SAFE. 109-113 basic network security topology, 113 *comprehensive network* security topology, 116–117 modest network security topology, 114–115 security wheel, 280-281 improve component, 287-288 change implementations, 289 policy adjustments, 288 monitor component, 284-285 data collection, 285 IDSs (intrusion-detection systems), 285 IPSs (intrusion-prevention systems), 285

network vunerability scanners, 287 retention, 285 secure component, 281-282 authentication, 282 encryption, 283 firewalls, 283 vunerability patching, 283-284 test component, 286 auditing, 287 responsibility determination, 286self-defending networks, 96 NAC (network admission control), 97 SA (Security Agent), 96 senior management consulting, 177-178 security incidents, effects on, 190 security requirements, assessing, 188-194 sensors, IPS sensors, training, 82 servers access control servers, 106-107 ACSs (access control servers), 71 authorization servers, 71 policies, 266-268 syslog servers, 95 service level agreements (SLAs), 158.296 session hijackings, 37 session replays, 38 short-term risks, 203-204 signatures, 49 single-loss expectancy (SLE). See SLE (single-loss expectancy), 220 site-to-site encrypted VPN, 61 Slammer worm, 99–100 SLAs (service level agreements), 158.296 SLE (single-loss expectancy), 220-223 asset-value estimations, 221 exposure factor, 222 smart cards, 69

sniffing, 25 social engineering, 33-36 software, 48 authorization and licensing, 248 AV (antivirus) software, 48-50 AV engines, 49 using multiple brands, 50 installation policies, 248 policies, 126, 273 custom software, 126-127 operating systems, 273 user software, 274-276 vendor-based software, 126-127 virus protection, 273–274 software exploitation, 27, 37 SSH (secure shell), remote configuration policies, 256 SSL (secure sockets layer) encryption, 63-65 remote configuration policies, 256 standby firewalls, 116 stateful failover. 116 stateful firewalling, traffic filtering, 55 - 58static biometrics, 70 steering committee opportunities, determining, 299-301 secure cultures, creating, 131-132 security initiatives, 154-155 strengths, determining, 297-298 threats, determining, 301-302 weaknesses, determining, 298-299 strong authentication, 68-70 PINs (personal identification numbers), 70 static biometrics, 70 tokens, 69 bio-tokens, 71 USB tokens, 71 strong passwords, 251-252

support, lobbying, IT management, 176-188 switches, 107 as invasion targets, 41-42 port security, 54 traffic filtering basic traffic filtering, 53–54 PVLANs (private virtual LANs), 53 SWOT (strengths, weaknesses, opportunities, and threats), 296-297 opportunities, 299-301 strengths, 297-298 threats, 301-302 weaknesses, 298-299 syslog servers, 95 syslogs, 94 system penetration attacks, 104

### Т

tagging, inventory control, 129–130 target-based IDSs, 82-83 targets, attacks, 104–105 TCO (total cost of ownership), equipment, 225-227 testing component, Cisco security wheel, 286 auditing, 287 responsibility determination, 286 "The State of Information Security 2003 Survey", 308 threads, attack threads, 28-29 threat mitigation, 96 APM (automated patch management), 98-100 NBAR (Network-Based Application Recognition), 97 self-defending networks, 96 NAC (network admission control), 97 SA (Security Agent), 96 technologies, 106

#### threats

application layer attacks, mitigating, 108 awareness levels, 4 determining, steering committee, 301-302 DoS attacks, mitigating, 106 IP spoofing, mitigating, 107 man-in-the-middle attacks, mitigating, 107 network reconnaissance attacks, mitigating, 107 packet sniffers, mitigating, 107 password attacks, mitigating, 107 port redirection attacks, mitigating, 108 RA (risk aversion) quotient, 204 calculating, 205 risk tolerance equivalency scale, 206 recognizing, 4 risk aversion, 200-201 risk exposure, lowering, 105-108 risk tolerance, determining, 202-203 risks, 203-204 targets, 104-105 trends, 104-105 Trojan horses, mitigating, 108 trust exploitation attacks, mitigating, 108 unauthorized access attacks, mitigating, 107 viruses, mitigating, 108 war-dialers, mitigating, 106 worms, mitigating, 108 three-strike access rules, 25 ticket assignments, assessment tools, 92 tokens bio-tokens, 71 passwords, 68 strong authentication, 68-69 USB tokens, 71 tools, policy tools, 245-246

topologies (security), 108–109 mapping, 15

SAFE, 110-113 basic network topology, 113 comprehensive network topology, 116–117 modest network topology, 114-115 security modeling, 207-210 law of diminishing returns, 213 - 214requirement management, 211-213 topology standards, 207–209 total cost of ownership (TCO), 225-227 traffic efficacy, routers, 260 traffic filtering, 50-51 advanced filtering, 55 proxy servers, 55 stateful firewalling, 55-58 basic filtering, 51 routers, 51-53 switches, 53-54 equipment, 59 training, IPS sensors, 82 trends, attacks, 104-105 Trojan horse attacks, 28, 37 threat mitigation technologies, 108 trust exploitation attacks, 26, 37 threat mitigation technologies, 108

# U

unauthorized access attacks, 104 threat mitigation technologies, 107 unsecured devices, vunerabilities, 6 unsecured user accounts, vunerabilities, 6 URLs (uniform resource locators), filtering, 83–84 outgoing-traffic administration, 85–87 tools, 84–85 USB tokens, 71 user compliance, policies, 135–136 user software, policies, 274–276

# V

vendor-based software, policies, 126 - 127virus protection, AV (antivirus) software, 48-50, 273-274 virus scans, 248 viruses, 28, 37, 104 signatures, 49 threat mitigation technologies, 108 VPN concentrators, 107 encryption, 63 VPNs (virtual private networks) encrypted VPN, 60-63 authentication, 62 confidentiality, 62 hashing, 62 integrity, 62 remote user, 61 secure data exchanges, 62 site-to-site, 61 VPN concentrators, 63 policies, 257 vunerability patching, Cisco security wheel, 283-284 vunerability scanners, Cisco security wheel, 287 vunerability scans, assessment tools, 90 vunerable points, acknowledging, 161-162

# W–Z

walk-by hacking, 38 wireless intrusions, 32 war dialers, policies, dialup and analog policies, 253–254 war driving, 30–31 war-dialers, threat mitigation technologies, 106 weak passwords, characteristics, 251 weaknesses, determining, steering committee, 298-299 white-hat hackers, 90-91 wireless intrusions, 30, 38-39 DoS (denial of service) attacks, 32 drive-by spamming, 32 eavesdropping, 30-31 frequency jamming, 33 man-in-the-middle attacks, 31 walk-by hacking, 32 wireless policies, 263-265 wokflow, policies, accounting for, 142 workforce, business relationships, building, 157–158 World Wide Web, network policies, 263 worms, 27-28, 37, 99 Mydoom worm, 100 propagation, 99-100 Slammer worm, 99-100 Stopping, NBAR (Network-Based Application Recognition), 97 threat mitigation technologies, 108