

Index

• *Symbols and Numerics* •

3G networks, 21, 177
4G/LTE networks, 21, 177

• *A* •

access control. *See* granular access control
access control policies, 74
access denied policies, 82, 83
access policies, 22, 25
access restricted policies, 82, 83
Active Directory (AD), 153
Address Space Layout Randomization (ASLR), 101
Afaria, Sybase, 281
agents, device, 54–55, 195, 206
aging, password, 112
AirWatch, 279
alarms, remotely activating device, 70, 136, 238, 239, 240
Android devices
backing up data, 250
backup and restore applications, 86
encryption, lack of, 132
versus iOS, 16–17
loss and theft protection on, 239, 242
number of apps for, 224
restoring data to, 255
sandboxing on, 267–268
transferring data between, 258
Wi-Fi policies for, 186
Wi-Fi networks, connecting to, 182–183
Android Market, Google
malicious applications in, 100
number of application in, 98
overview, 16
phishing applications on, 121
screening processes, 120
spam-only applications, control of, 48
Antidote, SektionEins, 101
antimalware protection, 135
antiphishing, 194–195
antispam protection, 135, 196–197, 210, 221, 222

antispymware, 159, 191–193
antitheft services, 234
antivirus software, 135, 158, 193–194, 210, 218–220
Anti-X protection
antiphishing, 194–195
antispam, 196–197
antispymware, 191–193
antivirus, 193–194
on-device, 190
APIs (Application Programming Interfaces), 16
App Genome project, 40
App Store, Apple
app security breach in, 40
downloading applications from, 16
malicious applications in, 100
number of application in, 98
publication of apps through, 15
screening processes, 120
spam-only applications, control of, 48
App World, BlackBerry, 62, 98, 241
Apple App Store. *See* App Store, Apple
Apple iOS operating system, 15–17, 235–237, 241–242, 266–268
Apple iPad. *See* iPad, Apple
Apple iPhone. *See* iPhone, Apple
application control, 120–123
application management, 69–70
application policies, protecting devices with, 97–101
Application Programming Interfaces (APIs), 16
application stores, 116, 120–121, 122, 223–225.
See also specific application stores by name
applications. *See also* malware; provisioning
access control, 161–163
adult usages of, 42
appeal of smartphones due to, 11
blacklisting, 125
client/server, 23–24
control of, 120–123
controlling and monitoring, 190, 201–202
e-mail, 23
increased use of, 60–62
messaging, 23

- applications (*continued*)
 - mobile security, 50
 - restricting installation of, 142
 - sandboxing. *See* sandboxing
 - standalone, 24
 - web-based, 23
 - applications catalogs, 122
 - approved applications, white-list of, 98
 - approved devices, policies for, 82
 - ASLR (Address Space Layout Randomization), 101
 - assessment, strategy, 27–28
 - AT&T Smart Limits, 196, 221
 - attachment downloads, restricting, 99
 - attack surfaces, 215
 - attack vectors, 22, 37
 - Aurora Feint application, 100
 - authentication
 - choosing VPN solutions based on, 73
 - dual-factor systems, 172
 - granular access control, 71–72
 - on-device security components, 200
 - policies for, 65, 71
 - for VPNs, 133, 152–154
 - authorization, 65, 72, 152, 154–155
 - auto-answer feature, malicious use of, 229
 - automated correction, 206–207
 - automatic syncing with Android, 250
 - automatic upgrades/downgrades, 96
- **B** •
- backup and restore policies, 69–70, 85–88
 - backups
 - on Android devices, 250
 - on BlackBerry devices, 251–252
 - capabilities of devices, 190, 197–199
 - corporate compliance policies, 139–141
 - corporate solutions for, 259–260
 - on iPhones and iPads, 249–250
 - loss and theft protection with, 234
 - on Nokia devices, 252–253
 - prior to upgrades or downgrades, 89
 - restoring data from, 254–257
 - from smartphones, 247–248
 - transferring data to new devices, 257–259
 - on Windows Phone 7 devices, 253–254
 - bada operating system, Samsung, 21
 - base OS, 268
 - battery life, effect of antivirus software on, 135
 - BES (BlackBerry Enterprise Server). *See* BlackBerry Enterprise Server (BES)
 - BlackBerry Enterprise Server (BES)
 - Black Hat DC 2010 conference, 100
 - BlackBerry Desktop Manager, 251–252, 256, 258
 - BlackBerry devices
 - backup and restore capabilities, 197–198, 251–252
 - centralized management console, 138
 - loss and theft protection on, 241, 243
 - management model for, 62, 128
 - number of apps for, 224
 - remote-wipe feature, 95
 - restoring data to, 256
 - sandboxing on, 265
 - transferring data between, 258
 - VPNs not needed for, 133
 - Wi-Fi networks, connecting to, 183–184
 - BlackBerry Enterprise Server (BES)
 - application policies, 99
 - application security policies, 265
 - backup and restore capabilities, 197–198, 252
 - centralized management console, 138
 - configuration and application management, 69
 - deployment policies of applications, 62
 - loss and theft protection with, 243
 - overview, 18, 28
 - W-Fi policies, 186
 - BlackBerry Protect application, 86, 87, 241
 - blacklisting applications, 122–123, 125
 - bluejacking, 117
 - Bluetooth security, 20–21, 117, 159, 214–215, 216
 - botnet membership, 192
 - browsers, location-aware browsing controls on, 52
 - brute-force ping floods, 218
 - bulk pricing, 204

• **C** •

 - calendars, access to, 164–165
 - cameras, disabling, 117
 - carrier selection, 204
 - CAs (certificate authorities), 153–154
 - catalogs of applications, 122
 - centralized management, 138–139
 - CERT, 278
 - certificate authentication, 71, 72, 133
 - certificate authorities (CAs), 153–154

- certificate revocation lists (CRLs), 154
 - certificates, machine, 160
 - client-based endpoint security software, 66–67
 - clientless VPNs, 166–167
 - client-only monitoring approach, 202
 - client/server applications, 23–24, 167–171
 - clipboard operations, controlling, 117
 - cloning, phone, 41
 - cloud computing, 62–63, 140
 - cloud storage apps, 43–44
 - cloud-based anti-phishing approach, 195
 - cloud-based security, 67–68
 - communications, hacked, 41–42
 - Commwarrior virus, 215
 - complexity, password, 112
 - compliance, 49, 206–208. *See also* corporate compliance policies
 - computers, back up on, 248
 - configuration files, deployment of, 109
 - configuration management, 69–70, 138–139
 - configuration policies
 - device functionality, restricting, 116–118
 - encrypting data, 114
 - network settings, 114–116
 - password policies, 111–114
 - removing prohibited applications, 114
 - configuration utilities, 109
 - connectivity options, 26
 - consumer application stores. *See* application stores
 - consumer e-mail accounts, restricting access to, 117
 - contact information stickers, 84
 - contacts, access to, 164–165
 - contract lengths, 204
 - corporate compliance policies
 - backups, 139–141
 - encryption, 131–132, 143–144
 - loss protection, 136–137, 145
 - managing devices at scale, 137–139
 - monitoring and controlling contents of devices, 141–143
 - operating system compliance, 143
 - passcodes, setting, 129–131
 - password compliance, 143
 - personal versus corporate-owned devices, 128–129
 - theft protection, 136–137, 145
 - virus protection, 134–135
 - VPNs, requiring, 132–134, 144
 - corporate-owned devices
 - backup and restore policies for, 85–86, 87–88
 - backups, compliance policies for, 141
 - centralized management, compliance policies for, 139
 - decommissioning policies, 94–95
 - encryption, compliance policies for, 132
 - loss and theft protection, compliance policies for, 137
 - malware, compliance policies for protection against, 135
 - monitoring and control, compliance policies for, 143
 - monitoring policies, 95–97
 - network access control for, 156–157
 - passcodes, compliance policies for, 131
 - versus personal devices, 128–129
 - profile settings policies, 91–94
 - VPNs, compliance policies for, 134
 - CPU utilization by security software, 67
 - CRLs (certificate revocation lists), 154
 - Cryptographic Technology group, NIST, 277
 - custom VPN security policies, 160–161
 - cutting-edge devices, support for, 59–60
- D •
- Dark Reading website, 276
 - data connections, 21–22
 - decommissioning policies, 94–95
 - defensive postures, 50–55
 - deployment
 - dynamic, 168
 - of e-mail applications, 109
 - enterprise-wide loss and theft protection, 243–244
 - of smartphones onto networks, 13–14, 24–28
 - strategy for, 25, 203–204
 - Desktop Manager, BlackBerry, 251–252, 256, 258
 - device agents, 54–55, 195, 206
 - device configuration policies, determining, 25–26
 - device deployment, 203–204
 - device discovery, 204–205
 - device functionality, restricting, 116–118
 - device lock scans, 159
 - device lock timers, 164
 - Device Management Working Group, 118

- device policies
 - backup and restore, 85–88
 - physical device protection, 83–85
- device profiles. *See* posture profiling, device security
- device provisioning, 205
- device selection, 204
- device type scans, 158
- digital certificates, 153–154
- Digital Millennium Copyright Act, 39
- discovery, device, 204–205
- disk encryption, scans for verification of, 159
- display size, decreased security due to, 194
- downgrade policies, 89–91
- downloads
 - from Android Market, 16
 - from App Store, 16
 - restricting e-mail attachment, 99
 - of software, by IT department versus users, 63
 - of third-party applications, restrictions on, 116–117, 123
 - virus propagation through, 216
- drive-by attacks, 39
- Droid, Motorola, 12, 36, 43. *See also* mobile devices
- dual-factor authentication systems, 71, 172
- dynamic deployment, 168

• E •

- EAS (Exchange ActiveSync), 119–120, 164
- eavesdropping, electronic, 41
- education, user
 - general discussion, 53–54
 - SMS, safe use of, 226
 - unsecured wireless networks, use of, 225
- electronic eavesdropping, 41
- e-mail applications
 - access policies for, 72
 - access to, 162, 164–165
 - attachment downloads, restricting, 99
 - configuration files, deployment of through, 109
 - consumer, restricting access to, 117
 - general discussion, 23
 - popularity of, 11
 - spam in, 220
 - virus attacks, 216
- e-mail configuration profile, iPhone, 91, 92
- e-mail source headers, 194

- employee-owned devices
 - acceptance and planning for, 59–60
 - allowed device types, compliance policies for, 130
 - Android devices, loss protection on, 239
 - Apple iOS devices, loss protection on, 235–237
 - backup and restore policies for, 85–86
 - backups, compliance policies for, 141
 - Blackberry devices, loss protection on, 241
 - centralized management, compliance policies for, 139
 - versus corporate-owned devices, 128–129
 - encryption, compliance policies for, 132
 - loss and theft protection, compliance policies for, 137
 - malware, compliance policies for protection against, 135
 - monitoring and control, compliance policies for, 143
 - monitoring policies, 95–97
 - network access control for, 157
 - passcodes, compliance policies for, 131
 - profile settings policies, 91–93
 - provisioning policies, 89
 - sandboxing on, 269–270
 - Symbian devices, loss protection on, 237–239
 - VPNs, compliance policies for, 134
 - Windows devices, loss protection on, 240
- employees. *See* users
- encryption
 - of backed up data, 250
 - backups and restorations, using for, 141
 - compliance of, determining, 144
 - corporate compliance policies, 131–132, 143–144
 - of data at rest, 114
 - disk, scans for verification of, 159
 - enforceable, 190
 - full disk, 102
 - on iOS devices, 267
 - mail server, enabling for connections, 164
 - on-device security components, 200
 - of SMS, 41
 - SSL, 164, 179
 - Wi-Fi networks, 179
- endpoint security, 26, 63, 64, 74. *See also* security components, on-device
- end-user supported backup and restoration, 199

enforceable encryption, 190, 210, 227–230
 enforceable policies, 50–51, 79–81
 enforcement, compliance, 206–208
 enterprise application stores, 122
 enterprise management of mobile devices,
 190, 203–208
 Enterprise Mobility Management,
 McAfee, 281
 Enterprise Strategy Group security priorities
 study, 88
 enterprise-grade solutions for loss and theft
 protection, 241–243
 enterprise-owned devices. *See* corporate-
 owned devices
 EVO 4G, HTC, 43
 Exchange ActiveSync (EAS), 119–120, 164

• F •

Facebook app, 196–197, 217
 fat client applications, 23–24
 Find My iPhone app, 95, 235, 236
 Firefox, Mozilla, 52
 firewalls
 battery usage concerns of, 213
 BlackBerry devices, 265
 compliance policies, including in, 135
 dynamic adaptation to changing usage,
 214–215
 memory footprint of on-device, 212–213
 on-device, 210
 scans for verification of, 158
 form factors of devices, 10–14
 fragmentation, operating system, 16–17
 free applications, 36
 Fruit Mobile, 215
 F-Secure website, 276
 full client/server applications, access to,
 162–163
 full disk encryption, 102
 functionality, restricting device, 118–120

• G •

Gartner website, 282
 geolocation ability, protecting, 52, 134
 Good Mobile Control, Good Technology, 280
 Good Technology, 270, 280
 Google Android devices. *See* Android devices

Google Android Market. *See* Android Market,
 Google
 Google Android operating system, 17
 Google servers, 250, 255, 258
 GPS, locating lost devices with, 236, 238,
 239, 240
 granular access control
 of applications, controlling, 62
 authenticating users, 71–72
 authorizing users, 72
 calendar applications, 164–165
 with clientless VPNs, 166–167
 client/server applications, 167–171
 contact applications, 164–165
 e-mail applications, 164–165
 importance of, 65
 overview, 22
 planning for, 61
 VPN policy infrastructure, integrating with
 existing, 73–75
 web-based applications, 166–167
 GSM Association, 278
 GSM spam reporting service, 196, 222
 guest VM, 268

• H •

hackers
 apps, use of, 40
 jailbreaking, 38–40, 44–45
 unencrypted data available to in public
 places, 132
 unsecured wireless networks, use of, 225
 writing malware, 40
 heap overflow bugs, 39
 history, password, 112
 HP Palm webOS, 20
 HTC EVO 4G, 43
 HTTPS, using for mail server connections, 119
 hypervisors, 269

• I •

ICSA labs (International Computer Security
 Association), 277–278
 idle timeout setting, 113
 IMEI (International Mobile Equipment
 Identity), 160, 234
 immobilizing techniques, 200

- inactivity timers, 70
 - incorrect passwords, maximum number of, 113, 136
 - Infosecurity Network website, 276
 - insecure Wi-Fi networks, 178–179, 225–226
 - instant messaging, spam in, 220
 - integrity policy, mobile device, 159
 - International Computer Security Association (ICSA labs), 277–278
 - International Mobile Equipment Identity (IMEI), 160, 234
 - Internet, 165, 211, 275–278
 - intrusion prevention, 210, 212, 223–226
 - inventories, application, 123
 - inventory management, centralized, 138
 - iOS Enterprise Program, 122
 - iOS operating system, Apple. *See* Apple iOS operating system
 - iOSurface library bug, 39–40
 - iPad, Apple
 - backing up data, 249–250
 - restoring data to, 254–255
 - similarity to smartphones, 12–13
 - storage capacity of, 36
 - transferring data between, 257
 - W-Fi policies for, 185
 - Wi-Fi networks, connecting to, 180–182
 - iPhone, Apple
 - backing up data, 249–250
 - backup and restore applications, 86, 87
 - backup and restore capabilities, 197
 - cloud storage apps, 43–44
 - configuration profiles, 91–93
 - features of, 43
 - number of apps for, 224
 - restoring data to, 254–255
 - storage capacity of, 36
 - touchscreen interface, 12
 - transferring data between, 257
 - URL obfuscation on, 195
 - W-Fi policies for, 185
 - Wi-Fi networks, connecting to, 180–182
 - iPhone Configuration Utility, 185
 - iPods, Apple, 180–182
 - IPsec VPN Layer 3 network-extension clients, 168–169
 - IPsec VPNs, 74, 150–151
 - iTunes application, 86, 87, 249, 254–255, 257
- J •
- jailbreaking, 44–45, 51, 101, 129
 - JailbreakMe 2.0 website, 38–39
 - Juniper Networks, 277, 280
 - Junos Pulse application, Juniper, 144, 145, 241–242, 245–246
 - Junos Pulse Mobile Security Suite, Juniper Networks, 280
- K •
- Kaspersky, 238
 - known devices, 160
 - Koobface worm, 217
- L •
- laptops, 13–14
 - latency with cloud services, 68
 - Layer 3 clients, 168–170
 - LBS (location-based services), 46–48, 52
 - LDAP (Lightweight Directory Access Protocol), 153
 - legacy networks, 29
 - legal disclaimers, public Wi-Fi network, 182
 - Linux Operating System, 268
 - local authentication, 152–153
 - location, remotely finding device, 70, 201
 - location information spoofing, 192
 - location-based services (LBS), 46–48, 52
 - lock timers, device, 164
 - locking devices, remotely
 - Android devices, 239
 - immobilizing technique, 200
 - loss and theft protection, 70, 136
 - with Microsoft's My Phone service, 240
 - with MobileMe, 236
 - Symbian devices, 238
 - locking down corporate devices, 128
 - logging and reporting management, centralized, 138
 - Long Term Evolution (LTE) networks, 21, 177
 - loss and theft protection
 - Android devices, securing data on, 239
 - Apple iOS devices, securing data on, 235–237
 - applications, controlling and monitoring, 201–202

applications, identifying harmful, 202–203
 Blackberry devices, securing data on, 241
 corporate compliance policies, 136–137, 145
 deploying enterprise-wide, 243–244
 encryption and authentication techniques, 200
 enterprise-grade solutions for various platforms, 241–243
 example of, 145
 geolocation features, misuse of, 53
 immobilizing techniques, 200
 policy on, creating, 64
 precautions before loss, 233–234
 remediation and recovery, 190, 200–201
 remote management of, 70
 strategy for, planning, 26–27
 Symbian devices, securing data on, 237–239
 threats to, 34–35
 Windows devices, securing data on, 240
 LTE (Long Term Evolution) networks, 21, 177

• M •

Mac OS X, 13
 machine certificates, 160
 mail server, 126, 164, 165
 malicious applications. *See* malware
 malware
 on Android devices, 16
 Android Market, care when downloading from, 16
 application-monitoring function, identifying with, 202–203
 client-based mobile endpoint security software, 66–67
 cloud-based security, 67–68
 as free apps, 36
 general discussion, 134
 intrusion prevention, 223–225
 protecting devices from, 64
 sandboxing and threat of, 264
 SSH, deactivating with, 46
 voice recording, 45
 managed devices, 160
 management systems. *See also* mobile device management
 choosing devices to manage, 49
 Open Mobile Alliance Device Management, 118–120
 remotely controlling, 68–70
 at scale, corporate compliance policies, 137–139
 scaling, 138
 man-in-the-middle attacks, 23
 manual remediation, 207–208
 manual upgrades/downgrades, 90
 McAfee, 277, 281
 McAfee WaveSecure, 238
 MDM. *See* mobile device management
 MECS (Mobile Enterprise Compliance and Security), Mobile Active Defense, 280
 MeeGo operating system, 20
 memory, device, 35–36, 67
 memory footprints, 35
 messages on lost phones, remotely activated, 236, 237
 messaging applications, 11, 23
 Microsoft Exchange server, 164
 Microsoft My Phone service, 240
 Microsoft Windows, 12, 13, 67
 Microsoft Windows Mobile, 19, 240, 242–243
 Microsoft Zune software, 253–254, 256–257
 minimum password length, 112
 MMS (multi-media message service), 221
 Mobile Active Defense, 280
 mobile device management (MDM)
 backup and restore solutions, 260
 configuration policies. *See* configuration policies
 Gartner website, reports on, 282
 loss and theft protection with, 241
 for lost or stolen devices, 35
 OTA management. *See* OTA management overview, 68
 W-Fi policies, defining, 186
 Mobile Device Management, Tangoe, 282
 mobile device security policy, creating, 25
 mobile devices
 applications for, 22–24, 60–62. *See also* applications
 cloud computing, 62–63
 cutting-edge devices, support for, 59–60
 data connections, 21–22
 granular access control, enforcing, 70–75
 laptops, 13–14
 malware protection, 65–68
 managing device policies remotely, 68–70
 mobility policies, updating, 63–64
 netbooks, 13–14
 networking, allowing in, 24–28
 operating systems. *See* operating systems

mobile devices (*continued*)

overview, 57–58

smartphones, 10–12

tablets, 10, 12–13

Mobile Enterprise Compliance and Security (MECS), Mobile Active Defense, 280

Mobile Management, Symantec, 281

Mobile Recovery app, Verizon Wireless, 201

mobile security apps, 50

MobileIron, 281

MobileIron's Virtual Smartphone Platform, 241–242

MobileManager, Zenprise, 282

MobileMe, 236–237

mobility policies, updating, 63–64

MogoRoad application, 100

monitoring

applications for, 202

of devices, 141–143, 205–206

policies, creating effective, 95–97

Motorola Droid, 12, 36, 43. *See also* mobile devices

Mozilla Firefox, 52

multifactor authentication, 65, 71–72, 153

multihomed mobile devices, 37

multi-media message service (MMS), 221

My Phone service, Microsoft, 240

• N •

National Institute of Standards and

Technology (NIST) website, 276–277

netbooks, 13–14

networks

access policies for, 72

configuring settings for, 115–116

dynamic access control, 156

example of settings for, 125

intrusion prevention, 225–226

online and offline modes for, 20–21

smartphone deployment onto, 13–14, 24–28

threats to, 36–37

NIST (National Institute of Standards and Technology) website, 276–277

Nokia devices

backing up, 252–253

personal, protecting from loss and theft, 237–239

restoring data to, 256

transferring data between Symbian devices, 259

Nokia PC Suite application, 252–253, 256

Nokia Symbian operating system, 19–20

notifications of critical events, 138

• O •

obfuscation, URL, 194, 195

OCSP (Online Certificate Status Protocol), 154

offline devices, 22

off-site data storage, 35–36

OMA Device Management (DM), 118

on-device agents, 195, 206

on-device Anti-X protection, 190–197

on-device security

components of. *See* security components, on-device

sandboxing, combining with, 270–271

one-time passwords (OTPs), 71, 133, 153

ongoing management process, 110–111

online application catalogs, 122

Online Certificate Status Protocol (OCSP), 154

online devices, 20

Open Mobile Alliance Device Management, 118–120

open Wi-Fi networks, 178–179, 225–226

operating system fragmentation, 16–17

operating systems

Apple iOS, 15–17

compliance of, determining, 143

corporate compliance policies, 143

Google Android, 17

HP Palm webOS, 20

MeeGo, 20

Microsoft Windows, 19

Nokia Symbian, 19–20

for notebooks, 13–14

RIM BlackBerry, 18

RIM BlackBerry Tablet, 18

Samsung bada, 21

for smartphones, 10–11

on smartphones and computers, differences between, 59

virtualization, 268–269

OTA (over the air) management

application provisioning, 121

device disabling, 199

initial provisioning workflow, 107–109

ongoing management, 110–111

OTPs (one-time passwords), 71, 133, 153

• P •

passcode profile, iPhone, 91, 92
 passcodes, in corporate compliance policies, 129–131
 password policies
 accepting new devices and, 144
 authentication, 71
 bad practices, 152
 complexity policies, 164
 corporate compliance policies, 143
 example of, 102, 123–124
 importance of, 70
 loss and theft protection with, 234
 overview, 111–114
 remotely controlling, 64
 strength of, 152
 password-aging policy, 112
 patched mobile devices, network access control for, 156–157
 PC Suite application, Nokia, 252–253, 256
 permissions, Android OS, 268
 personal devices. *See* employee-owned devices
 personal firewalls, 158, 265
 phishing, 47, 121, 194
 phone cloning, 41
 physical device protection policies, 83–85
 pilot groups, deployment to, 27
 policies. *See* specific policies by name
 policy lifecycle, five stages in IT, 80–81
 port forwarding, 170
 port scanning attacks, 218
 porting, 67
 posters, mobile security, 53–54
 posture profiling, device security
 access based on, 160
 custom policies, 160–161
 profiling devices and applying policies, 157–159
 postures, 50–55
 pricing, bulk, 204
 private APN (access point name), 114–116
 private cloud, 62
 profile settings policies, 91–94, 98–99
 profiling, device. *See* posture profiling, device security
 prohibited applications, removing, 114
 Protect app, BlackBerry, 241
 provider-supported backup and restoration, 199

provisioning, 121–122, 205
 provisioning policies
 decommissioning policies, 94–95
 profile settings policies, 91–94
 software installation policies, 89–91
 provisioning workflow, OTA management, 107–109
 proxies, 194
 proxy approach to ActiveSync traffic, 165
 public cloud, 62
 push notification, 107, 139, 185

• R •

radio interfaces, 37
 RADIUS (Remote Authentication Dial-In User Service), 153
 RDP (Remote Desktop Protocol), 60
 recovery techniques, 200–201
 reevaluation of strategies, 27–28
 remedial operations, 84–85
 renunciation, manual, 207–208
 remote access network, 171–175
 Remote Authentication Dial-In User Service (RADIUS), 153
 Remote Desktop Protocol (RDP), 60
 remote device security, 68
 remote lockdown, 200
 remote recovery, 84–85
 remote wipes. *See* wipes, remote
 removable media access, restricting, 117, 125
 removing applications, 114, 122–123
 replacement of lost/stolen devices, 34–35
 reporting management, centralized, 138
 requests for proposals (RFPs), creating, 27
 Research In Motion (RIM). *See* RIM (Research In Motion)
 restorations, data
 to Android devices, 255
 to BlackBerry devices, 256
 capabilities of devices, 190, 197–199
 corporate solutions for backup and, 259–260
 to iPhones and iPads, 254–255
 to Nokia devices, 256
 to Windows Phone 7 devices, 256–257
 restricting apps, 142
 restricting attachment downloads, 99
 rewriters, 167
 RFPs (requests for proposals), creating, 27
 Rick Astley wallpaper, 45, 46

- RIM (Research In Motion)
 - BlackBerry OS, 18
 - BlackBerry Tablet OS, 18
 - risks
 - in communications, 41–42
 - corporate data, endangering, 42–46
 - education on, 25
 - hackers, 38–41
 - location-based services, 46–48
 - rooted devices, rejecting on network, 129
- S •
- SAML (Security Assertion Markup Language), 154
 - Samsung bada operating system, 21
 - Samsung Vibrant, 43
 - sandboxing
 - on Android operating system, 17, 267–268
 - Apple iOS devices, 266–267
 - BlackBerry devices, 265
 - on employee-owned devices, 269–270
 - heap overflow bugs, breaking out of with, 39
 - importance of, 263–264
 - in iOS, 17
 - IOSurface library bug, breaking out of with, 39–40
 - on-device security, combined with, 270–271
 - virtualization for mobile devices, 268–269
 - SANS (SysAdmin, Audit, Network, Security), 275
 - scans of devices, 157–159, 160–161
 - screen captures, restricting, 117
 - screen size, decreased security due to, 194
 - SD cards, restricting access to, 117
 - SDK (software developer kit), 15
 - secure location, 52–53
 - Secure Shell (SSH), deactivating malware with, 46
 - security alerts, 194
 - Security Assertion Markup Language (SAML), 154
 - security components, on-device
 - antispam, 220–222
 - antivirus. *See* antivirus software
 - Anti-X protection. *See* Anti-X protection
 - backup and restore capabilities, 197–199
 - enforceable encryption, 227–230
 - enterprise management of devices, 190, 203–208
 - firewalls, 211–215
 - intrusion prevention, 223–227
 - loss and theft protection, 199–203
 - overview, 189–190, 209–210
 - Security Management and Assurance group, NIST, 277
 - security policies. *See also* configuration policies
 - application policies, protecting devices with, 97–101
 - device policies. *See* device policies
 - enforceable, recognizing importance of, 79–81
 - example of, 103–104
 - monitoring policies, creating effective, 95–97
 - provisioning policies. *See* provisioning policies
 - remote control of, 64
 - VPN, 157–161
 - security software, 135
 - security threat summaries, F-Secure, 276
 - security tokens, authentication using, 71
 - semi-automated correction, 207
 - Seriot, Nicolas, 100
 - server-based monitoring approach, 202
 - service provider assistance, for antispam protection, 221
 - short message service (SMS). *See* SMS (short message service)
 - SIM policies, 159
 - SIM snooping, 201
 - single-device policies, updating, 63
 - Smart Limits, AT&T, 196, 221
 - smartphones. *See also* mobile devices
 - backing up data from, 247–248
 - device agents, 54–55
 - general discussion, 10–12
 - SMS (short message service)
 - anti-spam solutions for, 196
 - encryption of, 41
 - hacking, 41–42
 - online and offline modes for connections, 20–21
 - OTA management with, 107
 - security apps for, 50
 - spam in, 47, 221
 - spyware manipulation of, 191–192, 226–227
 - text-to-voice applications, 202–203
 - virus attacks, 216

- social network applications, 53, 197, 217, 220–221
- software. *See also* antivirus software; applications
 installation policies, 89–91
 software developer kit (SDK), 15
- sounds on lost phones, remotely activated, 236
- source headers, e-mail, 194
- spam
 antispam solutions, choosing, 222
 general discussion, 134
 GSM spam reporting service, 222
 LBS based, 46–47, 52
 overview, 220–221
 service provider assistance for, 221
 SMS-based, 47
- spam-only applications, 48
- spoofing, location information, 192
- spy phones, 192
- spyware, 226–227
- SSH (Secure Shell), deactivating malware with, 46
- SSL encryption, 164, 179
- SSL VPN Layer 3 network-extension clients, 169–170
- SSL VPN Port forwarding client applications, 170
- SSL VPNs, 74, 166–167, 173
- standalone applications, 24
- stickers, contact information, 34
- storage capacity of devices, 36
- Storm8, 100
- Switch program, Nokia Symbian devices, 259
- Sybase, 281
- Symantec, 277, 281
- Symbian devices, 19–20, 237–239, 242, 259.
See also mobile devices
- synchronization, deployment of configuration files with, 109
- SysAdmin, Audit, Network, Security (SANS), 275
- Systems and Emerging Technologies Security Research group, NIST, 277
- T •**
- tablets, 10, 12–13. *See also* mobile devices
- TaintDroid application, 96
- Tangoe, 282
- Tech SANS website, 275
- tethering, 214
- text-to-voice applications, 202–203
- theft protection. *See* loss and theft protection
- third-party applications
 for BlackBerry devices, testing of, 265
 restrictions on downloads of, 116–117, 123
 security, prohibition by Apple on iOS, 15
 vulnerability of to hackers, 65
- threats
 defensive postures, 50–55
 risks. *See* risks
 scope of, 34–37
 tools for dealing with, 48–50
- timeout settings, 113
- timers
 device lock, 164
 inactivity, 70
- tokens, authentication using, 71
- touchscreen interface, 11, 12
- traffic, secure tunnel for, 67
- training, user, 53
- transferring data between devices, 257–259
- Trend Micro website, 277
- Trojans, 134
- typing errors, exposure to phishing due to, 194
- U •**
- UMA (Unlicensed Mobile Access), 184
- unapproved devices, policies for, 82
- United States Computer Emergency Readiness Team (US-CERT), 278
- unlocking versus jailbreaking, 38
- unsecured wireless networks, 194
- upgrade policies, 89–91
- URL obfuscation, 194, 195
- US-CERT (United States Computer Emergency Readiness Team), 278
- users
 backup and restore information, access to, 140–141
 educating. *See* education, user
 identity validation on VPNs, 151–155
 lost or stolen phones, recovery actions by, 136–137
 notification of application policy violations, 99
 software downloading policies, 63

• U •

vendor supported backup and restoration, 199
 vendors, mobile security, 27, 277, 279–282
 Verizon Wireless Mobile Recovery app, 201
 Vibrant, Samsung, 43
 violations, user notification of policy, 100
 virtual device solutions, 193, 219–220
 virtual machines (VMs), 269
 Virtual Network Computing (VNC), 60
 virtual private networks. *See* VPNs
 Virtual Smartphone Platform, MobileIron, 241–242, 281
 virtualization for mobile devices, 268–269
 virus signatures, updating, 66, 135
 viruses, 64, 134–135, 215–220
 VMs (virtual machines), 269
 VMWare, 268, 269
 VNC (Virtual Network Computing), 60
 voice recording malware, 45
 VPN connections, 133
 VPN profile, iPhone, 91, 93
 VPNs (virtual private networks)
 access, providing users appropriate. *See* granular access control
 allowing new devices on, 144
 application access, 161–163
 configuring settings for, 114–116
 corporate compliance policies, 132–134, 144
 discriminating by device profile. *See* posture profiling, device security evaluation of, 26
 IPSec versus SSL, 150–151
 overview, 149–150
 policy infrastructure, integrating granular access control, 73–75
 user identity validation, 151–155
 on Wi-Fi networks, 180

• W •

wallpaper, Rick Astley, 45, 46
 warranty terms for device replacement, 204
 WaveSecure, McAfee, 238
 web servers, deployment of configuration files on, 109
 Websites, security information, 275–278
 web-based applications, 23, 72, 121, 162, 166–167
 Weinmann, Ralf-Philipp, 229
 WEP (Wired Equivalent Privacy), 179

white-list of approved applications, 98
 Wi-Fi networks
 configuring settings for, 114–116
 connections from mobile devices, 180–184
 encryption, 179
 insecure, 178–179
 online and offline modes for connections to, 20–21
 open, 178–179
 overview, 177–178
 phishing attacks through usecured, 194
 policies for, 184–186
 VPN on, 180
 Wi-Fi policies, 184–186
 Wi-Fi Protected Access (WPA), 179
 Wi-Fi Protected Access 2 (WPA2), 179
 Windows, Microsoft, 12, 13, 67
 Windows Mobile, 19, 240, 242–243
 Windows Phone 7
 backing up, 253–254
 Connector application, 253
 loss and theft protection on, 240, 242–243
 number of applications for, 98
 overview, 19
 restoring data to, 256–257
 W-Fi policies for, 186
 wipes, remote
 Android devices, 239
 definitions of, 137
 Exchange ActiveSync protocols, 164
 with Find My iPhone app, 95
 immobilizing technique, 200
 loss and theft protection, 70, 136
 with Microsoft's My Phone service, 240
 with MobileMe, 236
 Symbian devices, 238
 Wired Equivalent Privacy (WEP), 179
 WLAN (wireless local area network), 116
 worms, 134
 WPA (Wi-Fi Protected Access), 179
 WPA2 (Wi-Fi Protected Access 2), 179

• X •

X.509 certificate authentication, 153–154

• Z •

Zenprise, 282
 Zune software, Microsoft, 253–254, 256–257