

Index

Numerics

802.1x, 153

A

AAA (authentication, authorization, and accounting), 33–35, 131
 accounting, 34, 154
 authentication, 150
 authorization, 153–154
 deploying technology, 149–150
 first factor, 151
 fourth factor, 152
 second factor, 151
 third factor, 152
 ABA (American Banking Association), 1
 acceptable use policies, 101
 process components, 121
 account administration, 100
 process components, 114–116
 adaptive management, 213
 administration
 people, 69–71, 82–83
 business units, 93
 facilities, 92
 Human Resources, 91
 Information Security
 Governance Board, 89–90
 information security organiza-
 tions, 84–85
 IT department, 91
 legal department, 91
 organizational structure, 86–88
 segregation of duties, 88

processes, 101–103, 123–124
 consistency, 125
 future processes, 125–127
 measuring compliance, 124
 setting examples, 124
 technology, 132–134
 anti-virus update programs, 168–169
 change management, 171
 future technology architecture, 171–172
 independent program review, 167
 program measurement, 169–170
 scanning and remediation, 166–167
 administrative access, 154
 alerts, 162
 American Banking Association. *See* ABA
 anomaly detection, 39, 207
 anti-virus software, 37–38, 159
 anti-virus update programs, 168–169
 appliances, versus server-based solutions, 144
 application intrusion prevention, 212
 application layer firewalls, 36
 application lockdown, 212
 application security, 209, 212
 architecture
 people, 93–95
 strategy groups, 88
 technology, 135
 assessment of information security, 179–182
 assets, identifying threats to, 106–108
 ATMs (Automated Teller Machines), 1
 attacks, information security attacks, 9–12
 auditing, security, 77
 authentication, 150
 protocols, 152
 wireless technology, 142

INDEX

authentication, authorization, and
 accounting. *See* AAA
 authorization, 34, 153–154
 automated lockdown, 208, 213
 automated patching, 208
 Automated Teller Machines. *See* ATMs
 availability, 177

B

baseline assessment, 47
 conducting, 53
 best of breed, 143–144
 biometric authentication, 152
 black hats, 80
 blended threats, 37, 196, 221
 BS (British Standard), 77–99, 67
 business environments, 59–61
 business models, 145
 business objectives, 46
 formal information security programs, 48
 business requirements, 56
 business environments, 59–61
 formal information security programs,
 49–50
 strategic objectives, 56–58
 summary of, 63
 tactical issues, 61–63
 business units, 93

C

California Senate Bill 1386, 19
 certification programs, 78–79
 Certified Information Security
 Manager. *See* CISM
 Certified Information Systems Auditor. *See* CISA
 Certified Information Systems
 Security Professionals. *See* CISSP
 change management, 171
 Chief Information Security Officer. *See* CISO
 CISA (Certified Information Systems Auditor), 15
 CISM (Certified Information Security
 Manager), 15, 77
 CISO (Chief Information Security Officer), 27
 CISSP (Certified Information Systems Security
 Professionals), 15, 77
 Class I threats, 198
 Class II threats, 198–199
 Class III threats, 199
 client/server/gateway security, 206, 209
 clients, 31, 131, 141
 compliance, 208
 PDAs, 142–143

Common Body of Knowledge, 77
 common logging, reporting, and alerting, 164
 communication, 99
 process strategies, 113
 complexity of threats, 195–197
 compliance
 and audit groups, 88
 measuring with process administration, 124
 components
 evaluating for formal information
 security programs, 50–51
 of processes, 100–101
 people, 67–68
 certification programs, 78
 credentials, 77–78
 employee training, 79
 good guys, 82
 hackers, 81
 hiring and developing your team, 75–78
 optional mix of staff, 79–82
 security auditing, 77
 security management, 76
 staffing challenges, 80
 technical staff, 76
 processes
 acceptable use policies, 121
 account administration, 114–116
 emergency response, 117–119
 remote access, 122–123
 security awareness, 116–117
 vulnerability management, 119–120
 technology 131–132, 143–146
 security technology categories, 147
 conducting baseline evaluations, 53
 confidentiality, 177
 consistency, process administration, 125
 content filtering, 40
 correlated application intrusion prevention, 212
 correlation, 164
 of security products, 213
 credentials, 77
 CISA, 78
 CISM, 77
 CISSP, 77
 GIAC, 78
 CRM (Customer Relationship Management), 31
 cross product correlation, 213
 cross-functional information security
 governance board, 219–220
 Customer Relationship Management (CRM), 31
 cyber terrorism, 202

INDEX

D

dashboards, 214
 data analysis, 164–165
 data management, (information security), 205
 day-to-day security operations, 88
 DDoS (Distributed Denial of Service)
 attacks, 196
 defense-in-depth, 26, 31–32, 139
 clients, 141–143
 gateways, 140
 servers, 141
 Denial of Service (DoS) attacks, 196
 deploying technology
 AAA, 149–150
 anti-virus software, 159
 firewalls, 156–158
 identity management, 155–156
 IDS, 161
 vulnerability management, 160
 designing processes, 104
 identifying threats to assets, 106–107
 risk assessment, 108–110
 security risk analysis, 104–106
 vulnerabilities, 108
 developing teams, 75–78
 digital gateway, 31
 digital zones, 131, 135
 extranets, 137–138
 intranets, mission critical zones, 138
 securing labs for nonproduction
 activities, 139
 directory services, 150, 156
 Distributed Denial of Service (DDoS)
 attacks, 196
 Documents, information security
 architecture documents, 54
 DoS (Denial of Service) attacks, 196
 dynamic mode (heuristics), 207

E

e-commerce, 6–8
 EDI (electronic data interchange), 145
 educating employees about processes, 113
 electronic commerce. *See* e-commerce
 electronic data interchange (EDI), 145
 electronic zones of defense, 32
 email subscriber lists, 175
 emergency response, 101
 process components, 117–119
 employees
 educating about processes, 113
 training, 79

encryption, 41
 enterprise information security program
 people, 26
 processes, 28–29
 technology
 AAA, 33–35
 anti-virus software, 37–38
 content filtering, 40
 defense-in-depth, 31–32
 encryption, 41
 firewalls/VPNs, 35–36
 intrusion detection, 39
 vulnerability management, 38
 technology, 29–30
 enterprise information security program, 26
 Enterprise Resource Planning. *See* ERP
 environments
 business environments, 59, 61
 ERP (Enterprise Resource Planning),
 12, 26, 31, 203
 European Data Protection Directive, 17
 evaluating formal information security
 program components, 50–51
 events, 162
 examples
 of Information Security Asset Inventory, 229
 of Information Security Business
 Dependency Matrix, 235
 of Information Security Existing
 Program Evaluation Summary, 234
 of Information Security Gap Analysis, 237
 of Information Security Risk
 Assessment Summary, 230
 of Information Security Roadmap, 239
 of Information Security Strategic
 Alternatives, 238
 of process administration, 124
 Extensible Mark-Up Language (XML), 211
 extranets, digital zones, 136–138

F

facilities, 92
 organizations, 83
 false positives (heuristics), 207
 financial institution collapse, 217
 firefighting mode, 131
 firewalls, 156–158
 application layer, 36
 OSI model, 157
 packet filtering firewalls, 35
 proxy-based, 36
 stateful inspection, 35
 first factor authentication, 151

INDEX

flash threats, 197
 forensics, 166
 formal information security programs
 business requirements, 49–50
 evaluating components, 50–51
 leveraging gap analysis, 51–52
 formal information security programs, 48–49
 fourth factor authentication, 152
 FTC (Federal Trade Commission), 17
 functional information security
 organizations, 86
 future of information security, 194

G

GAMMA GUPPY, 25
 gap analysis, 48, 183, 185
 formal information security
 programs, 51–52
 gateway/server/client security, 206, 209
 gateways, 140
 servers, 31
 geographic information security
 organizations, 87
 GIAC (Global Information Assurance
 Certification), 15, 78
 GLBA (Gramm-Leach-Bliley Act), 18
 Global Information Assurance
 Certifications (GIAC), 15, 78
 Global Positioning System (GPS), 152
 good guys, 82
 government legislation, 16–20
 GPS (Global Positioning System), 152
 Gramm-Leach-Bliley Act (GLBA), 18
 gray hats, 80
 guidelines
 for developing information security architec-
 ture documents, 54
 for successful information security
 programs, 23

H

hackers, 3, 81
 hardening, 166
 Health Information Portability &
 Accountability Act (HIPAA), 18
 heuristics, 38, 207
 HIPAA (Health Information Portability
 & Accountability Act), 18
 hiring teams, 75–78
 history of Internet, 3–6
 HRIS (human resources information system), 115
 HTTP (Hypertext Transfer Protocol), 211
 Human Resources, 91

human resources information system (HRIS), 115
 Hypertext Transfer Protocol (HTTP), 211

I

identifying threats to assets, 106–107
 identity management, 150
 deploying technology, 155–156
 IDS (Intrusion Detection Systems), 39, 161
 IETF (Internet Engineering Task Force), 158
 improvement of information security program,
 2, 20, 222–223
 in-house versus outsourcing, 72–74
 incidents, 162–163
 naming conventions, 97
 independent reviews of information
 security program, 167, 221
 industry regulations, 16–20
 compliance, 74–75
 industry-recognized certifications, 67
 information overload, 162–163
 information security, 2
 architecture documents, 54
 assessment of, 179–182
 program assessment scoring, 236
 asset inventory example, 229
 attacks, 9–12
 business dependency matrix, 60,
 181–182, 225, 235
 compliance issues, 67
 data management, 205
 e-commerce, 6–8
 evaluation framework, 179–180
 gap analysis, 183–185, 237
 government legislation and industry regula-
 tions, 16–20
 guidelines for success, 23
 hierarchy, 13
 immaturity of information security
 market, 12–14
 incidents, 2, 5
 MyDoom, 11
 Trojans, 9
 life cycle, 47
 market, 12–14
 mobile workforce and wireless
 computing, 20–22
 organizations, 84–85
 processes. *See* processes
 program technology, firewalls, 156–158
 risk analysis, 104
 roadmap, 176–179, 239
 shortage of information security staff, 14–16
 strategies, 46–47, 186–188, 238

INDEX

Information Security Analyst, 248–249
 Information Security Auditor, 249–252
 Information Security Director, 245–247
 Information Security Existing Program
 Evaluation Summary, 234
 Information Security Future People
 Architecture template, 227
 Information Security Future Process
 Architecture template, 231
 Information Security Future Technology
 Architecture template, 233
 Information Security Governance Board, 89–90
 Information Security People Evaluation
 template, 226
 Information Security Risk Assessment
 Summary example, 230
 Information Security Technology
 Evaluation template, 232
 Information Systems Audit and Control
 Association (ISACA), 77
 integrity, 177
 intellectual property. *See* IP
 interior deployments, 157
 internal versus external firewall deployment, 156
 Internet, history of, 3–6
 Internet Engineering Task Force (IETF), 158
 intranets, 31, 136
 digital zones, mission critical zones, 138
 securing labs for nonproduction
 activities, 139
 intrusion detection, 39
 Intrusion Detection Systems. *See* IDS
 intrusion prevention, 205–207
 investment in information security
 program, 185, 188
 IP (intellectual property), 10
 ISACA (Information Systems Audit and Control
 Association), 77
 IT organizations, 91
 information security organizations, 85

J-K-L

Kerberos, 153
 knowledge transfer, 73

 labs, securing for nonproduction, activities, 139
 layered security, 221–222
 layering, 31
 least privilege, 177
 legal department, 91
 leveraging gap analysis for formal information
 security programs, 51–52
 life cycles of information security, 47

M

malicious code, viruses, 9
 measuring process administration compli-
 ance, 124
 Melissa Virus, 198
 methodologies, 47–48
 conducting baseline evaluations, 53
 formal information security programs
 business requirements, 49–50
 evaluating components, 50–51
 leveraging gap analysis, 51–52
 formal information security
 programs, 48–49
 security evaluation framework, 52–53
 success factors, 55
 metrics, 166, 170, 220
 mission critical zones, 31, 136–138
 mobile workforce, 20–22
 Morris Worm, 4
 MyDoom, 11

N

naming conventions, incidents, 97
 need-to-know basis, 28
 ninety-day tactical plan, 61–62
 nonproduction activities, securing labs, 139
 normalization, 164

O

operational standards, 244
 organizational structure, 86–88
 OSI model, firewalls, 157
 Outsourcing versus in-house, 72–74
 ownership of information security
 program, 218–219

P

packet filtering firewalls, 35
 patching, 166–167
 PDAs, defense in depth, 142–143
 penetration testing, 132
 people
 administration, 69–71, 82–84
 business units, 93
 facilities, 92
 human resources, 91
 Information Security Governance
 Board, 89–90
 information security organizations, 84–85
 IT department, 91
 legal department, 91

INDEX

- organizational structure, 86–88
- segregation of duties, 88
- architecture, 93–95
- components
 - certification programs, 78
 - credentials, 77–78
 - good guys, 82
 - hackers, 81
 - hiring and developing your team, 75–78
 - optional mix of staff, 79–82
 - security auditing, 77
 - security management, 76
 - staffing challenges, 80
 - technical staff, 76
- components, 67–68, 75, 79
- enterprise information security
 - program, 26–28
 - strategies, 66–67, 71
 - in-house versus outsourcing, 72–74
 - industry regulation, 74–75
 - key decisions, 71–72
- perimeter, 135
- phishing, 193
- Ping-of-Death, 39
- pings, 39
- PKI (Public Key Infrastructure), 41
- point solutions, 203
- policies, acceptable use policies, 121
- principle of least privilege, 28
- privacy, 16
- proactive threat solutions, 204–205
- processes
 - administration, 101–103, 123
 - consistency, 125
 - future processes, 125, 127
 - measuring compliance, 124
 - setting examples, 124
- components, 100–101
 - acceptable use policies, 121
 - account administration, 114–116
 - emergency response, 117–119
 - remote access, 122–123
 - security awareness, 116–117
 - vulnerability management, 119–120
- designing, 104
 - identifying threats to assets, 106–107
 - risk assessment, 108–110
 - security risk analysis, 104–106
 - vulnerabilities, 108
- enterprise information security
 - program, 28–29

- strategies
 - communication, 113
 - considerations for, 112–113
 - strategies, 99–100, 111–112
- programs
 - enterprise information security, 30
 - people, 26–28
 - processes, 28–29
 - technology, 29–30
 - enterprise information security program, 26
 - formal information security programs
 - business requirements, 49–50
 - evaluating components, 50–51
 - leveraging gap analysis, 51–52
 - formal information security programs, 48–49
 - measuring, 169–170
- protocols, authentication, 152
- provisioning, 150
- proxy-based firewalls, 36
- Public Key Infrastructure (PKI), 41

Q-R

- quickly spreading threats, 197–199

- RADIUS (Remote Authentication
 - Dial-In User Service), 153
- remediation, 166–167
- remote access, 34, 100
 - process components, 122–123
- Remote Authentication Dial-In User
 - Service (RADIUS), 153
- Request for Comments (RFC), 158
- Requirements. *See* business requirements
- RFCs (Request for Comments), 158
- risk analysis, 104–106
- risk assessment, designing processes, 108–110
- roadmap. *See* information security roadmap, 179
- roles
 - of Information Security Analyst, 248–249
 - of Information Security Auditor, 249–252
 - of Information Security Director, 245–247
- router throttling, 207
- routers, 158

S

- Safe Harbor Agreement, 17
- SANS (SysAdmin, Audit, Network Security), 76
- Sarbanes-Oxley Act, 19
- scanning, 166–167
- scoring, Information Security Program
 - Assessment Scoring, 236
- second factor authentication, 151
- Secure Sockets Layer. *See* SSL

INDEX

securing labs for nonproduction activities, 139
 security. *See* information security
 security auditing, 77
 security awareness, 101
 process components, 116–117
 security domains, 77
 security evaluation framework, 52–53
 security forensics, 166
 security management, 76, 161–162
 data analysis, 164–165
 forensics, 166
 information overload, 162–163
 security risk analysis
 designing processes, 104–106
 security solution management, 212–214
 security technology categories, 147
 security tokens, 138
 segregation of duties, 68, 88
 self-replicating, 37
 senior-level staff responsibility for
 information security program, 219
 server-based solutions versus appliances, 144
 server/client/gateway security, 206, 209
 servers, 141
 gateway servers, 31
 shortages of information security staff, 14–16
 signature-based recognition, 39, 206
 signatures, 206
 virus signatures, 37
 Simple Object Access Protocol (SOAP), 211
 simplification of threat solutions, 203–204
 single-sign-on, 150
 Slammer Worm, 199
 smart cards, 202
 SOAP (Simple Object Access Protocol), 211
 Software, anti-virus software, 37–38, 159
 SSCP (System Security Certified Practitioner), 15
 SSL (Secure Sockets Layer), 41
 staffing challenges, 80
 stateful inspection firewalls, 35
 static mode (heuristics), 207
 stealing email subscriber lists, 175
 strategic alternatives (information security), 186, 188
 strategic objectives, business requirements, 56–58
 strategies
 people, 66–67, 71
 in-house versus outsourcing, 72–74
 industry regulation compliance, 74–75
 key decisions, 71–72
 processes
 communication, 113
 considerations for, 112–113

processes, 99–100, 111–112
 technology, 130–131, 134
 best of breed, 143–144
 business models, 145
 defense in depth, 139–143
 integrated solutions, 143–144
 server-based solutions versus appliances, 144
 success factors for methodologies, 55
 SysAdmin, Audit, Network Security (SANS), 76
 System Security Certified Practitioner (SSCP), 15

T

tables

Changing Attacker Demographics, 81
 High-Level Information Security Metrics, 170
 Information Security Asset Inventory, 105
 Information Security Business Dependency Matrix, 60
 Information Security Future People Architecture, 94
 Information Security Future Process Architecture, 126
 Information Security Future Technology Architecture, 172
 Information Security People Evaluation, 70
 Information Security Process Evaluation, 103
 Information Security Risk Assessment Summary, 110
 Information Security Roles and Responsibilities, 83
 Information Security Technology Categories, 147
 Information Security Technology Evaluation, 133
 Major Information Security Threats, 107
 tactical issues, business requirements, 61–63
 teams
 hiring and developing, 75–78
 security auditing, 77
 security management, 76
 technical staff, 76
 technology
 administration, 132–134, 166
 anti-virus update programs, 168–169
 change management, 171
 future technology architecture, 171–172
 independent program review, 167
 program measurement, 169–170
 scanning and remediation, 166–167

INDEX

components, 131–132, 143–146
 security technology categories, 147
 deploying
 AAA, 149–150
 anti-virus software, 159
 firewalls, 156–158
 identity management, 155–156
 IDS, 161
 vulnerability management, 160
 designing for future, 134
 enterprise information security program
 AAA, 33–35
 anti-virus software, 37–38
 content filtering, 40
 defense in depth, 31–32
 encryption, 41
 firewalls/VPNs, 35–36
 intrusion detection, 39
 vulnerability management, 38
 enterprise information security
 program, 29–30
 strategies, 130–131, 134
 architecture, 135
 best of breed, 143–144
 business models, 145
 defense in depth, 139–143
 digital zones, 136–139
 integrated solutions, 143–144
 server-based solutions versus
 appliances, 144
 wireless technology, defense in
 depth, 142–143
 templates
 Information Security Future
 People Architecture, 227
 Information Security, Future
 Process Architecture, 231
 Information Security Future
 Technology Architecture, 233
 Information Security People Evaluation, 226
 Information Security Process
 Evaluation, 228
 Information Security Technology
 Evaluation, 232
 third factor authentication, 152
 threats
 evolution, 194–200
 identifying, 106–107
 traffic, 131
 Trojans, 9
 two-factor authentication, 33

U-V

U.S. Federal Trade Commission (FTC), 17
 U.S. National Security Agency, 25

 virtual private networks. *See* VPNs
 virtual sandboxes, 38
 virus throttling, 208
 viruses, 9
 anti-virus software, 37–38
 signatures, 37
 visualization, 164
 VPNs (virtual private networks), 35–36
 Vulnerabilities, identifying when designing
 processes, 108
 vulnerability management, 38, 101
 process components, 119–120
 technology, 160
 vulnerability-threat window, 200

W

“Warhol Worms: The Potential for Very Fast
 Internet Plagues” (Weaver), 198
 Weaver, Nicholas, 198–199
 web services, 211
 wireless computing, 20–22
 wireless technology, defense in depth, 142–143
 worms
 Morris Worm, 4
 Slammer Worm, 1–2

X-Y-Z

XML (Extensible Mark-up Language), 211

 zero-day attacks, 200
 zones, 222