

Index

Symbols

4-step plan 338

A

access control 219
 activity theory 282
 ad hoc computing 426
 administrative ROBAC 103
 anonymity techniques 218
 Anshin, structure investigation 498
 Anshin in system design 497
 anti-phishing toolbar 261
 antiphishing education, designing 257–278
 antiphishing toolbars 178
 AntiPhishing Working Group (APWG) 177
 APPEL 214
 attack cycle 233
 attack techniques 234
 attack vectors 180
 auditing 238
 authentication 218
 authorization 219
 avoiding privacy policy pitfalls 152

B

bayesian belief networks (BBN) 66
 biometrics recognition systems 51
 biometric technologies 399
 BIOTRACKER 61
 browser plug-ins 178
 browser vulnerabilities 180
 business processes, modeling 13

C

catastrophe 6
 catastrophe, impact on security and privacy 7
 catastrophe contingency planning 13
 catastrophe contingency plans (CCPs) 1
 catastrophes, responsibilities and liabilities 1–22
 closed circuit television (CCTV) 50
 commercial auctions 466
 compound failures 18
 context-adapted privacy protection 480
 context-aware phishing attacks 260
 context-aware phishing IQ module 266
 context-free grammars 393
 context in security 198

Index

contingency failures, testing 18
contingency planning 5
contingency plans, developing 9
contradiction on computers, overcoming 400
contradiction on mobile devices, overcoming 402
copula 67
copula aided bayesian belief network (CBBN)
 model 64
cost of breach model 137
countermeasures, attacks 236
credit card, privacy, identity, and security 166
cross-site scripting (XSS) 180
crossover error rate (CER) 399, 408
cultural and behavioral shifting 29
curriculum process 295
cyber crime 249
cyber crime, nature of 434
cybercriminal, the rise 23
cyberworld, privacy 166

D

Digital Millennium Copyright Act (DMCA) 252
digital signing 178
disclose-to attribute 151
distributed cognition theory 283

E

e-commerce honesty-credit system, construction 83
e-commerce security 73–93
e-commerce security risk management strategy,
 problems 76
e-commerce transactions game model 79
e-learning education, traditional 350
e-learning environment 351
e-learning environment, information security
 346–362
e-learning information security measures 358
e-learning information security pillars 352
e-risk 65, 66
e-risk insurance product design 64–72
e-risk quantification (E-RQ) 69
e-service model 144
e-vulnerability analysis (E-VA) 68
education, training, and awareness (ETA) 237
educational websites 263
electronic voting 427
emergency response 20
employee surveillance 47–63
employee surveillance technologies 50
encryption vs. steganography 381

enterprise functionality 119
enterprise information security engineering lifecycle
 126
enterprise information system 120
enterprise information system security 118–132
enterprise information system security, need for 120
enterprise information system security, problems
 121
enterprise information system security parameters
 123
enterprise privacy authorization language (EPAL)
 215
equal error rate (EER) 399
extensible access control markup language (XAC-
 ML) 216
external privacy policy language 212

F

false acceptance rate (FAR) 399
false information overflowing 78
financial damage 263
fine-grained security solutions 198
forensics 302
four step plan 338
free text detection of keystroke dynamics 47–63

G

general deterrence theory 285
graphical authentication protocols 403
grounded theory 286

H

hackers 250
hardware tokens 179
honest-credit, defined 74
honest-credit, study 75
honesty-credit 73–93
honesty-credit environment, construction 90
honesty-credit problems, reasons 81
human-computer interaction security 417
human attack in linguistic steganography 380–397
Human Reliability Assessment (HRA) 415

I

identity and access management (IAM) 135
identity in banking 165
identity management 218
image site keys (ISK) 262
information assurance, meeting SIGITE guidelines
 293–306

information security 4
 information security, limitations 308
 information security, new world of 23–46
 information security, policies and procedures 347
 information security, technical and non-technical 348
 information security, theory application 280
 information security at large public displays 471–492
 information security awareness 197, 307–324, 349
 information security awareness, making it more effective 316
 information security awareness, trends 319
 information security awareness, value and need 312
 information security governance 349
 information security investment, alternative model 133–141
 information security objective 26
 information security research 279–292
 information states 302
 insider threats 49
 insider threat study (ITS) 49
 internal privacy policy language 215
 Internet crime 433–445
 Internet crime, influencing factors 436
 Internet crimes, vulnerability 435
 ISO 27001 security standard 330
 IT security spending, modeling 135

J

joint accounts 170

K

keystroke dynamics 400
 keystroke dynamics recognition systems 54

L

large-volume tests 19
 large public displays, active privacy support 479
 large public displays, information security 471–492
 layered security 328
 learning model 332
 lexical steganography, past approaches 391
 linguistic steganography 381
 linguistic steganography, human attack 380–397
 Lunabel 383
 Lunabel, internal mechanics 387

M

malwares 250
 media 231
 minimum processes principle 198
 model-checking driven design 419
 model driven security 364
 money and privacy 164
 multi-day tests 19

N

new world of information security 26

O

online English auctions 447
 OOA07 model 110

P

passgraph, generating a password 406
 passwords, case 367
 personal space concept 480
 PETs, evaluating 211
 philanthropic phools 260
 phishing, diversity 258
 phishing attack detection, content based 179
 phishing attack detection, two stage approach 182
 phishing attacks, defending against 175–192
 phishing botnets 260
 phishing e-mails, structure 181
 phishing harms 263
 phishing IQ test 265
 PKI based schemes 178
 pointer dynamics 407
 policy-based privacy management 142–160
 PRA07 model 108
 prevention services 126
 privacy 5
 privacy, different approaches 163
 privacy-enhancing technologies (PETs) 203–227
 privacy-enhancing technologies, evaluating 207
 privacy and banking in Australia 161–174
 privacy concerns 54, 210
 privacy in the bank 168
 privacy landscape 205
 privacy laws and regulations 205
 privacy legislation 144
 privacy levels to control information 481
 privacy management, avoiding pitfalls 142–160
 privacy management model 145
 privacy management system 218

Index

- privacy policies 145
- privacy policies, application 147
- privacy policies, maintenance 147
- privacy policy languages 211
- privacy policy pitfalls 148
- privacy policy pitfalls problem 143
- privacy problem 142
- privacy problem, solving 143
- privacy rights management, design 171
- prospect theory 236
- psychological factoring 32

R

- recovery services 126
- recovery software 18
- regular contingency planning 10
- representativeness heuristic 236
- responsiveness in the bank 168
- return on security investments 368
- RFID readers 484
- ROA07 model 111
- ROBAC, applying to Web applications 113
- ROBAC models 99
- role-base access control (RBAC) 94
- role-based learning 333
- role and organization based access control (RO-BAC) models 94
- RRA07 model 109

S

- search engines, assurance issues 370
- security, areas of conflict 363–379
- security breaches, people based 326
- security curriculum 336
- security curriculum meeting the SIGITE guidelines 293–306
- security domains 303
- security education, training, and awareness program (SETA), creating 325–345
- security infrastructure advisory phase 129
- security in global partnerships 372
- security in interactive systems, analysis 415–432
- security in outsourcing 372
- security in the business environment 35
- security investments, return on 368
- security mechanisms (countermeasures) 298
- security policy formulation phase 127
- security protocols 426
- security requirement analysis 127

- security services 125
- security testing and validation 129
- security to resilience 39
- security usability 366
- sense of security 493–502
- sense of trust 493–502
- session hijacking attacks 180
- SETA program, creating one 336
- SETA program, effectiveness evaluation 342
- skill behavior 448
- skill bidding 446
- skill bidding in online English auctions 446–470
- skill characteristics and strategies 449
- skill detection 450
- skill mindset 448
- skill score 452
- skill score, calculating 459
- SIGITE guidelines 293–306
- social cognitive theory (SCT) 287
- social engineering, context profile 196
- social engineering, countermeasures 228
- social engineering attacks, a taxonomy 230
- social engineering impact, reducing 193–202
- social interactions, new paradigm 247
- social network analysis 32
- social networking for businesses 246
- social networking site 243–256
- social networking site, history 244
- social network theory 244
- socio-technical (STS) systems theory 281
- special interest group for information technology education (SIGITE) guidelines 294–306
- SPIROS, technical realization 483
- SPIROS architecture 484
- SPIROS privacy manager (SPM) 486
- SPIROS scanner manager (SSM) 485
- steganography, defined 381
- surveillance society 43
- system for privacy-enhanced information representation in open spaces (SPIROS) 483

T

- targeting 230
- team based access control (TMAC) 96
- third-party authentication 86
- third-party service providers 88
- threat analysis model 301
- true business benefit 36
- trust and Anshin, system design 497
- trust damage 263

U

UROA07 model 106

V

visual identification protocol (VIP) 404

vulnerabilities 300

vulnerability, dependent variables 439

W

watermarking 391

Web 2.0 250

Web safety 249

well-formed (WF) privacy policy 153

word replacement 392

X

XPref 214