

# Index

## A

adoption 119, 125, 127, 128, 134, 136,  
137, 395, 397  
anger retaliatory 55  
Association of American Railroads (AAR) 269  
asymmetric warfare 116, 407  
attacker 42, 43, 44, 372, 374  
attack graph 23, 37, 45, 46, 386, 398, 407  
attack surface 40, 46, 403  
attestation 351, 355, 358, 360, 368, 411  
auditing 49, 58, 61, 63, 66, 126, 133, 188,  
195, 196, 236, 243, 244, 245, 288,  
331, 334, 335, 336  
autocorrelation function  
77, 81, 85, 86, 88, 92  
autocorrelation methodology 76, 77, 80, 82,  
85, 94, 95  
automated attacks 379

## B

best practices 48, 50, 61, 79, 120, 121,  
122, 125, 138, 165, 199, 203, 253,  
311, 315, 316, 403  
black market 2, 3, 4, 5, 8, 10, 12, 13, 15,  
16, 19, 20, 22, 387, 409  
bootstrap 90, 91, 93  
bottleneck 263, 278, 285

## C

centralized server model 321  
climate 211, 214, 221, 227  
cognitive dimension 141, 142, 144, 152,  
154, 156, 157, 158  
collaboration engineering 250, 251, 252,  
253, 258, 259, 260, 262  
community 9, 11, 16, 17, 123, 186, 197,  
236, 283, 296, 303, 307, 308, 309,  
310, 311, 312, 313, 314, 315, 316,  
320, 344, 372  
Computer Network Defense (CND)  
203, 217, 389  
confidentiality 294, 295, 296  
congestion 266, 267, 268, 269, 273, 277,  
278, 279, 304  
container port operations 267  
content analysis 290, 291, 292, 294, 295,  
300, 414  
contingency theory 201, 202, 205, 207, 214,  
215, 216  
control analysis 58  
control recommendations 60  
core root of trust measurement (CRTM) 353  
culture 62, 98, 111, 115, 117, 161, 193,  
384, 388, 397, 415  
cyber-forensics 379

## **Index**

cyber security 50, 235, 266, 280, 303, 307,  
308, 309, 233, 309, 308, 309, 310,  
311, 312, 313, 314, 315, 316

## **D**

daemons 322, 323, 324, 325, 326, 332  
daily total times to resolve (DTTR) 77  
data smog 157, 158  
decentralized server model  
321, 322, 323, 330  
digital privacy rights management (DPRM)  
179  
disaster management organizations (DMO)  
284  
distraction 151  
dummy information 380

## **E**

e-business 251  
economics of information security 20, 22, 72,  
388, 396, 410, 414  
electronic commerce 72, 182, 183, 367, 368,  
369, 389, 398, 400, 409, 414, 416  
emergency 8, 51, 70, 204, 212, 218, 237,  
249, 286, 300, 301, 303, 304, 307,  
311, 316, 322, 384, 388, 408, 417  
emergency response 99, 285, 286, 287, 291,  
293, 294, 298, 315  
endorsement key (EK) 354, 355, 356  
expert system 217, 385  
exploit 29

## **F**

fair information practice principles (FIPP) 167  
flexible encryption 377  
fog & friction 142, 143  
freight transportation 265, 266, 268, 278,  
279, 280  
full disclosure 8, 9, 11, 21, 22, 397, 404,  
411

## **H**

Honeypot 371, 372, 373, 374, 375, 376,  
377, 378, 379, 380, 381

honeytokens 68  
human resources 61, 185, 266, 267, 279

## **I**

identity keys 354, 355  
impact analysis 59, 251  
incident response 251, 252, 254, 257, 260,  
262, 250, 262, 255, 260, 261, 262,  
264, 303, 307, 308, 312, 313, 379,  
395, 418  
information assurance 79, 96, 165, 186, 193  
, 195, 198, 217, 233, 235, 283, 284,  
294, 297, 298, 364, 389, 390, 412  
information operations 117, 141, 142, 144,  
155, 162, 163, 202, 217, 392, 400,  
417, 418  
information overload 146, 147, 155, 161,  
163, 387, 397, 413, 417, 418  
information quality dimensions 286  
information security 9, 10, 20, 21, 22, 55,  
70, 72, 73, 75, 76, 78, 80, 81, 82,  
85, 95, 96, 97, 99, 108, 110, 111,  
113, 116, 119, 120, 121, 122, 123,  
124, 125, 126, 127, 128, 129, 130,  
131, 132, 133, 134, 135, 136, 137,  
138, 139, 140, 167, 182, 184, 186,  
187, 188, 189, 190, 193, 194, 195,  
196, 197, 198, 199, 200, 217, 251,  
258, 284, 287, 293, 294, 297, 298,  
305, 337, 349, 356, 367, 368, 369,  
371, 372, 378, 380, 384, 385, 386,  
387, 388, 389, 390, 393, 395, 396,  
398, 399, 401, 402, 403, 404, 405,  
406, 407, 408, 409, 410, 411, 412,  
413, 414, 415, 417, 418, 419  
information sharing 121, 284, 285, 287,  
297, 300, 302, 307, 308, 283, 307,  
310, 311, 312, 313, 314, 315, 316,  
408, 410  
information supply chain 169  
information terrorism 97, 98, 101, 102,  
103, 107, 108, 109, 111, 113, 114,  
117, 418

information warfare 71, 97, 98, 99, 100, 101, 102, 103, 104, 106, 108, 109, 110, 111, 112, 113, 114, 117, 261, 386, 392, 394, 408, 418  
 insider 49, 50, 52, 53, 70, 71, 72, 73, 74, 384, 387, 388, 390, 399, 400, 401, 402, 403, 407, 409, 412, 415  
 insider attack 53, 58, 60, 62  
 insider threat 49, 53, 70, 71, 72, 73, 72, 73, 74, 384, 387, 388, 390, 399, 400, 401, 402, 403, 409, 415  
 integrity measurement, storage and reporting 350  
 intellectual property 74, 417  
 internal control 165  
 intrusion detection system 364, 372  
 ISO/IEC 27001 119, 123, 124, 125, 126, 129, 133, 134, 136, 137, 395, 397, 398  
 IT professionals 165, 180, 185, 186, 187, 188, 192, 196, 197

## L

lean media 143  
 likelihood determination 59  
 linear regression 92, 93

## M

malicious insider 73, 402  
 management 21, 45, 57, 60, 61, 62, 71, 72, 73, 74, 84, 95, 116, 117, 123, 125, 135, 136, 137, 138, 139, 146, 150, 154, 162, 169, 192, 193, 194, 196, 198, 213, 214, 217, 219, 221, 222, 225, 227, 228, 239, 241, 243, 244, 246, 247, 248, 97, 119, 181, 261, 248, 261, 281, 299, 300, 301, 302, 337, 339, 363, 365, 367, 368, 384, 385, 386, 387, 388, 389, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 416, 419  
 Maritime Administration 276, 282, 416

Marksteiner's corrolary 156  
 maturity model 308, 312, 313, 314, 315  
 Metcalfe's Law 143, 156, 161, 162, 396, 404  
 misfits 201, 210, 211, 218, 222, 224, 228, 230, 406  
 motivation 54, 136, 391, 392

## N

National Infrastructure Protection Plan 266, 279, 281, 416  
 national security 117, 186, 193, 198, 202, 217, 304, 338, 346, 363, 368, 390, 392, 406, 412, 418  
 new security environment 102, 116, 117, 398, 418

## O

observable 50, 64, 65, 68, 76, 130, 149  
 opportunistic 55  
 organizational change 129, 138, 213, 214, 215, 400  
 organizational consultant 205, 206  
 organization structures 203

## P

pandemic influenza 265, 266, 268, 274, 276, 278, 279, 280  
 personally identifiable information (PII) 164, 165  
 platform configuration register (PCR) 352  
 Port of Long Beach 267, 274, 275, 277, 280, 281, 409  
 Port of Los Angeles 267, 274, 275, 276, 277, 279, 280, 281, 409  
 power assertive 55  
 power reassurance 55  
 privacy rights 175  
 protected capabilities 350, 351  
 public policy 164, 166, 181, 182, 246, 385, 387, 399, 408

## Q

queuing 270, 274, 276, 305

**R**

railroad operations 268  
reference monitor 347  
regulation 174, 183, 243, 244, 412  
responsible disclosure 9  
results documentation 60  
rich media 147  
Rich Media Theory 147  
risk assessment 57, 243  
risk determination 59  
risk management 50, 56, 135, 136, 387, 394  
risk mitigation 23, 24, 26, 44, 48, 50, 56,  
59, 60, 61, 68, 295  
role expectations 184, 185, 186

**S**

secure server 328, 336  
security assessment 79  
security assurance 75, 76, 77, 78, 94, 95  
security assurance assessment 94, 95  
security certifications 135, 188, 198, 388  
security event 75, 76, 78, 82, 85, 86, 95,  
307  
security event management 76, 82  
security incident 76, 205, 262, 308, 377,  
418  
security infrastructure 75, 76, 77, 78, 80,  
82, 83, 84, 85, 86, 87, 89, 93, 94,  
184  
security metrics 76, 78, 79, 80, 81, 82,  
83, 94  
security policy 25, 53, 58, 61, 62, 66, 76,  
84, 121, 125, 134, 135, 137, 140,  
187, 190, 192, 196, 197, 253, 295,  
348, 350, 398, 418  
security researchers 6, 7, 8, 9, 11, 350  
security standard 135, 385  
server hardening 321, 322, 324, 325, 326,  
327, 332, 333, 334, 335, 336  
server hardening model  
327, 333, 334, 335, 336  
software vulnerabilities 1, 2, 6, 8, 9, 11,  
21, 400  
storage root key 354, 355, 356, 357  
system audit 66

system characterization 57  
system compromise 324  
system dynamics 22, 73, 403, 409

**T**

technical skills 190  
techno creep 143  
Threat 22, 26, 45, 49, 51, 53, 58, 70, 71,  
72, 73, 1, 23, 48, 72, 73, 74, 115,  
116, 146, 302, 338, 384, 387, 388,  
390, 397, 399, 400, 401, 402, 403,  
408, 409, 414, 415  
threat identification 26  
transformation plan 213  
trust 53, 73, 192, 194, 344, 345, 352, 353,  
355, 357, 358, 359, 364, 366, 367,  
389, 395, 400, 402, 403, 404, 413  
trusted computing 338, 343, 344, 346, 348,  
349, 350, 359, 361, 362, 364, 365,  
366, 367, 368, 367, 369, 343, 367,  
368, 369, 383, 389, 396, 399, 400,  
401, 406, 408, 411, 413, 416, 417  
trusted computing base (TCB) 348, 350  
trusted computing group (TCG) 343, 344,  
346  
trusted platform 343, 344, 350, 351, 352,  
353, 354, 355, 356, 358, 364  
trusted platform module (TPM) 343, 344, 350  
trusted software stack (TSS) 352  
tyranny of the convenient 150, 151  
tyranny of the urgent 153

**U**

U.S. Department of Homeland Security  
266, 267, 279, 281, 416

**V**

virtual machine monitor 346  
vulnerability 6, 7, 8, 10, 11, 15, 20, 25,  
43, 46, 58, 76, 93, 367, 382, 389,  
399, 400, 404, 409  
vulnerability black markets 3, 5  
vulnerability disclosure 8, 9, 10, 11, 20, 22,  
386, 388, 409  
vulnerability discovery 6

vulnerability identification 58  
vulnerability markets 8, 10  
vulnerability secrecy 8

**W**

worker absenteeism 265, 266, 267, 268, 277,  
278, 279, 280

**Z**

zero-day vulnerability 2