

Index

A

abilene 311-312, 314, 316, 323
 access complexity 200
 access vector 200
 action planning 291, 295
 action taking 291, 295
 Active Directory (AD) 222
 American Gas Association (AGA) 135, 149
 amplitude modulation (AM) 157
 anomaly detection 17, 19-20, 29-32, 39-42, 45-46, 48-50, 52, 128, 134, 352, 357-358, 365, 381-382
 anti-malware 222-223
 Apache 191, 195, 197-198, 201, 264
 arc 323
 audit and control association (ISACA) 270

B

BACnet 4-5, 7, 13
 Bluetooth 9, 162, 353
 border gateway protocol (BGP) 332
 bottom-up construction 252-253, 261
 Building Management Systems (BMS) 1, 4

C

carrier wave (CW) 157
 central office (CO) 51-52, 101, 103-104, 185, 260, 280, 305, 323, 380
 Centre for the Protection of National Infrastructure (CPNI) 112, 135, 281, 331
 cloud computing 113-114, 128, 138
 commercial off the shelf (COTS) 218, 220
 Common Platform Enumeration (CPE) 200, 213
 Common Vulnerability Enumeration (CVE) 199
 Common Vulnerability Scoring System (CVSS) 200, 326, 347
 communication protection 8
 communication protocol 158
 community-oriented critical information infrastructure protection 261
 Community-Oriented Security, Advisory and Warning (C-SAW) 253

Computer Security Incident Response Teams (CSIRTs) 214, 241, 247-253, 256, 260, 331
 confidentiality 113, 117, 123, 200, 227, 264-265, 279, 332-333, 337, 341, 350
 continuity of operations 9, 21, 286
 control centre 18-20, 32-33, 38-39, 41, 48, 84, 248
 Control Objectives for Information Technology (COBIT) 270
 Control Systems Security Program (CSSP) 115
 counter measure 209
 CRAMM 306, 323
 Critical Information Infrastructure (CII) 107, 262-263
 Critical Information Infrastructure Protection (CIIP) 240-242, 261, 327
 critical infrastructure (CI) 223
 Customer Relationship Management (CRM) 268
 cyberattack 21, 32, 40, 48-49, 85, 87, 90-91, 99, 102, 145, 156, 171-172, 174, 176-179, 181-182, 186-189, 217, 245, 252, 259, 265-267, 277, 282, 339, 346, 379
 cyber pilot 335
 cyber security 16, 18-19, 50-53, 82-84, 88, 90, 101-103, 107, 110-111, 116-118, 121, 125, 135, 137-138, 140-142, 148, 163, 165-166, 168-179, 181-186, 188-189, 203-205, 213, 215, 217-222, 234-235, 238-241, 246-248, 259, 267, 277-279, 290, 300, 302, 315, 319, 321, 325, 329, 335, 337, 339, 341, 344-346, 348-350, 352, 377-378
 cyber shockwave 176, 186
 Cyberspace Policy Review 173, 188-189
 cyberterrorism 176, 185, 189, 278
 cyberwar 113, 171, 177-178, 181-182, 184-186, 188, 268, 278, 280, 351

D

data acquisition framework 146, 150, 154, 157, 159, 162, 166
 Data Execution Prevention (DEP) 225
 data historians (DH) 51-52, 79, 87-88, 113, 137, 145, 164, 181, 184, 186, 228, 281, 319, 348, 350, 355, 378
 data network 6

defense industrial base (DIB) 335
 Denial of Service (DoS) 7
 Dependability Development Support Initiative (DDSI) 330
 deployment 9, 83, 117, 126, 135, 140, 150, 155, 160-161, 182, 201, 206-209, 240-241, 246, 251-252, 255, 284, 332, 354-355, 362, 376
 diagnosing 170, 291, 295
 diagnostic framing 177, 189
 Digital Agenda for Europe (DAE) 106
 disaster recovery plan 206
 distributed control systems (DCS) 27, 118, 142, 166, 197, 219-220, 353
 distributed monitoring system 145, 149-153, 158, 162, 167
 Distributed Network Protocol (DNP3) 167, 353
 distributed system 155
 DoD Cyber Crime Centre (DC3) 335
 Domain Name System (DNS) 330
 dynamic link libraries (DLL) 229

E

eavesdrop 148, 159
 economy 21, 58, 169, 172-177, 196, 231, 241, 250, 263, 302, 304, 324, 335, 338
 efficiency 3, 9, 12, 20, 53, 56, 58, 100, 102, 122, 124-125, 146, 154, 193, 203, 210, 244, 351, 362, 372
 electromagnetic pulse (EMP) 304, 319
 Electronic Content Management (ECM) 268
 Electronic Security Perimeter (ESP) 148
 Embedded Middleware-Level Intrusion Detection System (EMISDS) 359
 encrypted 115, 148, 230, 233
 Energy Management Systems (EMS) 3, 18
 Energy Star 5
 EnOcean 5
 Enterprise Resource Planning (ERP) 157, 268
 environmental security 8
 ethical hacking 14, 263, 272, 274, 279, 282
 European Network and Information Security Agency (ENISA) 84, 105-106, 263, 281, 333
 European Programme for Critical Infrastructure Protection (EPCIP) 106
 expectation maximization (EM) 357
 exploitability 200
 Exponentially-Weighted Moving Average (EWMA) 365
 extended Kalman filter (EKF) 357

F

fortify 303, 306, 308-311, 313, 323
 Freedom of Information (FoI) 340

G

Geographic Information Systems (GIS) 78
 global technology audit guidelines (GTAG) 270
 Google maps 78
 Government Accountability Office (GAO) 86

H

harmfulness 170, 177-178, 182-184, 189
 High Altitude Electromagnetic Pulse (HEMP) 304
 Home Area Network (HAN) 155
 human factor (HF) 83, 103, 164, 285, 289-290, 293, 297-298
 Human-Machine Interfaces (HMIs) 33, 144, 146, 158, 162, 167, 219, 221-223, 225, 228, 230, 232-233, 238

I

industrial control system (ICS) 19, 21-22, 50-51, 82-87, 91-92, 94, 100-103, 105-135, 137, 140, 142-143, 145-147, 151, 163-164, 166-167, 179-180, 187, 190-193, 195-199, 201-205, 207-224, 226, 228, 230-239, 259, 279, 299, 302, 353-354, 381
 information exchange (IE) 122, 135, 138-139, 155, 165, 253, 324, 328-345, 347-348, 351, 379
 information security 84, 102, 104-106, 115, 118, 137, 140-141, 143, 193, 199, 213-215, 263-265, 267-277, 279-285, 290, 292, 298, 300, 320, 328-329, 333, 336, 339-341, 345, 347-349, 351, 379, 381
 information security governance (ISG) 274
 Information Security Management System (ISMS) 118
 Information Technology Assurance Framework (ITAF) 270
 Information Technology Governance Institute (ITGI) 270
 insider attack 94, 359
 Intelligent Building (IB) 1-9, 12-16
 intelligent electronic device (IED) 18, 20, 23, 34, 36, 38-39, 138, 147, 158, 165, 220, 228, 237-239
 interdict 323
 Interface Definition Language (IDL) 359

Index

International Electrotechnical Commission (IEC)
138-139, 145, 149
International Monetary Fund (IMF) 241
Internet of Things (IoT) 162
Internet Protocol (IP) 315, 326, 330, 332
Intrusion Detection System (IDS) 153, 355

K

key risk indicator (KRI) 271-272, 277, 285

L

Linux 198, 220, 232, 237, 264
Local Area Network (LAN) 3, 18, 146, 219, 221
Logical Bomb 269
LonWorks 4-5, 7, 13, 29

M

Machine-to-machine (M2M) 158, 167
malware 21-22, 95, 102, 112-113, 117, 125, 137,
145, 176, 180-181, 184, 186, 191, 194-196,
207-208, 211, 218-226, 228-229, 239, 241,
245-248, 255, 260, 266, 353, 378
master control stations (MCS) 228
Master Terminal Units (MTU) 222, 228
McAfee 113, 140, 181, 187, 288, 299, 353, 377
Meter Data Management System (MDMS) 155
microgrid 154, 167
mitigation 1-2, 8-10, 15, 55-57, 60, 67, 70, 76, 78,
219, 223, 234, 263, 271, 283, 320-321, 326,
329-330, 334, 336-337, 343-344
motivational framing 170, 177, 182-183, 189
MySQL 197-198

N

National Cybersecurity and Communications Inte-
gration Center (NCCIC) 222
National Infrastructure Advisory Council (NIAC)
330
National Vulnerability Database 190, 194, 199, 208,
216
networked system 308
Network Security Information Exchange (NSIE)
331
Network Security (NetSec) 220
node 78, 85, 280, 302, 307, 309, 311-315, 317, 323,
359-360
non disclosure agreement (NDA) 272, 332, 340-341,
345
North American Electrical Reliability Corporation
(NERC) 148
Norwegian Computer Society (DnD) 294-295

O

Object Linking and Embedding (OLE) 353
OCTAVE 306, 318
Oil and Gas Industry Association (OLF) 293
Organization for Economic Cooperation and Devel-
opment (OECD) 177

P

Patch and Vulnerability Group (PVG) 206-207
patch evolution 202
patch information 202, 210
patch management 190-195, 198-199, 201-216, 275
personnel security 9, 76, 102, 274-275
Petroleum Safety Authority (PSA) 292, 294
physical security 1, 9, 15, 76, 80, 94, 116, 121, 131,
138, 141, 147
portable document file (PDF) 19-20, 24, 48-52, 101-
104, 135, 137-138, 140, 142, 163-164, 166,
186, 213-216, 223, 226, 229, 239, 243, 259-
260, 278-280, 299-300, 319, 346-350, 357, 378
precautionary principle 277
process control systems (PCS) 3, 23, 110, 138, 140-
141, 216, 220, 228, 246, 286-287, 304, 325,
346, 377
prognostic framing 182, 184, 189
Programmable Logic Controller (PLC) 23, 33, 110,
141-142, 145-147, 167, 197, 218, 220, 228,
232-233, 237, 287-288, 351, 353, 365
Public Private Partnerships (PPP) 122-123, 125,
130, 132, 328-329, 331, 333-334, 336, 346-
348, 351
Public Switched Network (PSN) 146

Q

Quality of Service (QoS) 128

R

Radio Frequency Identification (RFID) 144, 157,
167
reliability envelope 306
remediation level 200
remote procedure call (RPC) 227
remote terminal unit (RTU) 18, 20, 22-23, 31, 33-
34, 36-39, 41, 110, 146-147, 149, 165, 167,
220, 228, 232-233, 237, 287, 303
Remote Terminal Unit (RTU) 18, 20, 22-23, 31,
33-34, 36-39, 41, 110, 146-147, 149, 165, 167,
220, 228, 232-233, 237, 287, 303
return on security investment (ROSI) 277

risk assessment 55, 58-61, 70-71, 77, 102, 124, 164, 166, 206, 271-272, 286-293, 295-297, 306, 346
 risk impact 64
 risk management measure 64
 risk rating 64, 68-69
 Robust Generalized Likelihood Ratio Test (RGLRT) 352, 356
 rootkit 143, 145, 164
 Routine Activities Theory 95, 102, 104

S

safeguard 17, 29-31, 54, 56, 65, 174
 securitization 170, 182, 186, 189
 security awareness 1, 9, 15, 87, 186, 218, 230, 235, 249, 260, 274, 276, 293, 300
 security monitoring 130, 191, 208, 210, 214
 security risk management 1, 8, 15-16, 58-59, 75, 81, 273
 Sequential Hypothesis Testing (SHT) 363
 simulation support 78
 Single Points of Contact (SPoC) 333
 situational awareness 53, 149-150, 152, 156, 162, 165, 167, 226, 232-234, 377
 smart grid 16, 51-52, 114-115, 117, 123, 128-130, 133, 140-142, 144-145, 148, 153-160, 163-167, 214
 smartphone 162
 specify learning 291, 295
 stakeholder relationship 58
 Stuxnet 21-22, 49, 83, 112-113, 115, 137-138, 145, 164, 172, 178-181, 186-188, 190-191, 194, 214, 217-218, 221, 246-248, 260, 266, 268, 277-278, 280, 284, 288, 299, 324-325, 345, 347, 353, 365, 378, 381
 Stuxnet virus 83
 substation 20, 32, 34-36, 138, 147, 158, 165-166, 359
 Supervisory Control and Data Acquisition (SCADA) 17, 142, 144, 147, 165-167, 197, 218, 220, 299, 324, 352-353, 381
 systematic security, threat, risk, and vulnerability assessment (STRVA) 54
 System Operations Committee (SOC) 25

T

target distribution 200
 telecommunication service utilities 18
 test bed 106, 123, 132, 134, 137, 163
 threat assessment matrix 68
 threat object 189

top-down construction 261
 Trojan virus 89
 Trusted Computing Module (TCM) 237
 Trusted Information Sharing Network (TISN) 335
 Trusted Platform Modules (TPM) 231, 237, 239

U

USB stick 84, 93
 Utility Communications Architecture (UCA) 353

V

virtual machines (VM) 218-219, 230-231, 237, 239
 vulnerability 1-2, 4, 6-9, 14-15, 18, 21, 23, 29, 34, 48, 52-57, 60-61, 64-66, 71-72, 75, 77-82, 84-85, 87-88, 96, 99-101, 103, 109-111, 113, 125, 127-129, 133, 142, 152-153, 156, 159-161, 171, 173, 177, 179, 190-196, 199-203, 205-216, 222-223, 225-226, 229, 231, 234-235, 238, 241, 244, 247, 256, 258, 261-262, 264, 267, 269, 272-273, 275-279, 283-289, 292, 294, 296-297, 302, 306, 308, 311, 318-326, 329-333, 335-338, 340, 344-345, 347-349, 351, 353
 vulnerability assessment 54, 57, 60-61, 64, 80, 192, 208, 211, 272, 321
 vulnerability notification 205

W

Warning, Advice, and Reporting Point (WARP) 253, 261
 Web Application Firewalls (WAF) 142, 228
 whitelisting 138, 219, 228-229, 232, 238
 Wide Area Network (WAN) 18
 WiFi 9, 162, 353
 wireless 5, 7-9, 13, 15-16, 23, 33-34, 125, 128, 140, 150, 155-161, 163-167, 191, 198, 220-221, 232-234, 239, 243, 245-246, 264, 303, 305, 353, 357, 378, 382

Y

Y2K 263-264, 269

Z

ZigBee 5, 9, 140, 143-144, 154-155, 157-159, 161-162, 164, 166-167, 353
 ZigBee Device Object (ZDO) 159
 Zotob worm 83