

A

Accidental malfunction, 103
Accidents will happen, 143
Accumulation management, 251, 252, 253
Achieving malicious aims by abusing security systems, 90
Advanced persistent threats, 139
Allocation of capacity, 249
Alternative versions of the past 10 years of cyber attacks, 181
Amateur hackers, 14, 126, 127, 128
Amazon, 14, 69, 72, 74, 147, 338, 343, 350
Anatomy of a data exfiltration attack, 1
Anderson, Ross, 93, 277
Anomaly detection algorithms, 222
Anonymous, 134, 135, 353
Anticipate, withstand, recover, and evolve, 214
Antivirus, 48, 119, 174, 202, 207, 262, 291, 298
Arsenals of exploits, 104
Articulated damages, 194
Asymmetric encryption, 325.
See also Cryptography
ATM machines, 132, 199

B

Bangladesh National Bank, attack on via SWIFT, 66
Bank of America, 67, 271, 340
Beebone, 306, 350
Binary similarity, 304, 305
Binary similarity problem, 304
Bitcoin, 1, 44, 52, 53, 54, 55, 56, 147, 148, 177, 344
Botnet, 20, 42, 43, 49, 50, 57, 62, 117, 128, 133, 147, 149, 171, 173, 181, 202, 204, 263, 288, 291, 306, 350
Bounty, 174, 278–281, 283, 285, 286, 290, 291, 315, 345
 Zerodium, 282, 283
Brief history of cyber-physical interactions, 81
Bringing cyber criminals to justice, 290
Buffett, Warren, 250, 337, 338
Bug, 14, 29, 61, 73, 103, 104, 107, 110, 111, 121, 122, 157, 165, 174, 176, 177, 211, 228, 229, 230, 254, 257, 276, 277, 278, 279, 280, 281, 282, 283, 285, 286, 290, 291, 296, 297, 301, 302, 303, 304, 311, 315, 316, 335, 338, 344, 345, 350, 352
 vulnerability, 280

- Bug economic valuation, 278
- Bug-hunting businesses, 282
- Building back better, 230, 231
- Burning out power generators, 84
- Business continuity, 62, 97, 154, 156, 209, 210, 261
- Business continuity planning and staff engagement, 210
- Business interruption, 220, 235, 238, 239, 240, 242, 243, 244, 246, 255, 259, 274
- Byzantine Generals Problem, 93, 94, 343
- C
- Canal safety decision problem, 298
- Carbanak*, 65, 131, 132, 133, 340, 348, 352
- Carderplanet, 129
- Catastrophes, 12, 13, 14, 16, 17, 18, 23, 26, 27, 249, 250, 252, 254, 257
- Challenges of carrying out an extreme event, 173
- Change the display/induce operator error, 93
- Change the file and you change the world, 91
- Changing approaches to risk management, 207
- Characterizing extreme events, 172
- Chatbots, 20
- Chicago, 201
- Chief information security officer (CISO) 6, 154–158, 167, 172, 231, 233, 269, 271, 280, 292, 293, 339, 342
- CIA, 14, 204, 285
- Cisco Webex, 70
- CISO. *See* Chief information security officer (CISO)
- Citibank, 67, 340
- Class-action lawsuits, 195
- Clausewitz, Carl von, 178
- Cloud, 14, 15, 16, 31, 53, 69, 70–79, 164, 165, 229, 230, 253, 254, 255, 256, 257, 261, 333, 337, 338, 341, 343, 344, 348
- Cloud service providers (CSPs), 14, 69, 70, 71, 73–78, 164, 255
- Cocks, Clifford. *See* Government Communications Headquarters (GCHQ)
- Collecting information on cyber loss incidents, 24
- Common Vulnerability Scoring System (CVSS), 108, 110, 111, 115, 347
- Compliance and law enforcement, 196
- Compliance management, 198, 199
- Components of cyber-physical systems, 86
- Computer emergency response teams (CERTs), 106
- Computer science, 83, 86, 88, 100, 102, 119, 131, 295, 296, 322, 324, 348, 349

- Conficker*, 41, 42, 173, 181, 204, 291
- Consequential business losses from a cyber attack, 9
- Control the actuators, 91
- Cooperation of private sector with law enforcement, 201
- Correlation, 117, 248, 263 and insurance, 248
- Cost-effective technologies, 269
- Cost-effectiveness of security enhancements, 267
- Cost-effectiveness surveys, 268
- Costs of cyber attacks to the US economy, 25
- Counterfactual, 13, 29, 46, 178, 179, 180, 193, 230, 257, 339, 352
- Counterfactual analysis, 13, 46, 178, 230, 257, 352
- Cryptocurrencies, 18, 50, 52, 125, 147
- Cryptography, 96, 262, 281, 299, 321, 322, 324, 325, 326, 327
- CryptoWall, 53
- CSP outages, 71
- CVSS. *See* Common Vulnerability Scoring System (CVSS)
- Cyber attack economic multipliers, 10
- Cyber attacks and game theory, 283
- Cyber black economy, 128, 130, 134, 147, 337
- Cyber catastrophe, 12–18, 23, 26, 27, 31, 240, 245, 247, 248, 249, 252, 253, 254, 331, 336
- Cyber catastrophe risk, 248
- Cyber criminal, 55, 63, 65, 66, 104, 125, 126, 128, 129, 130, 132, 134, 142, 146, 147, 148, 156, 170, 174, 191, 200, 201, 231, 232, 278, 281, 284–287, 290, 292, 296, 298, 306, 307, 310, 312, 316, 317, 329, 341
- Cyber criminal's dilemma problem, 306
- Cyber criminology, 126, 146, 152, 335, 343
- Cyber events that could have turned out differently, 180
- Cyber extortion, 53, 54, 55, 238, 244
- Cyber extortion attacks on larger organizations, 53
- Cyber heists, 313
- Cyber hygiene, 196, 197, 211, 212
- Cyber insurance, 29, 164, 192, 193, 196, 226, 227, 235–265, 275, 333–337, 348, 349, 353
- Cyber insurance market, 193, 236, 244, 245, 246, 251, 258, 264, 265, 333, 349
- Cyber insurance underwriting, 249, 258, 260, 261
- Cyber laws, 183, 186
- Cyber litigation, 194
- Cyber loss processes, 33, 164, 257, 267
- Cyber loss ratio variation, 258
- Cyber ops, 20, 21

- Cyber-physical interactions, 81, 82
- Cyber risk analysis, 95, 179, 274, 296, 302–304
- Cyber risk awareness, 144, 210, 275
- Cyber risk levels across the world, 25
- Cyber safety, 329, 330
- Cyber security, 4, 29, 55, 66, 67, 99, 126, 143, 153, 155–159, 161, 163, 164, 166, 168, 170, 171, 185, 186, 188, 191–199, 204, 207, 208, 209, 211, 212, 214, 218, 220, 221, 222, 225, 227, 228, 232, 233, 246, 248, 251, 252, 260, 262, 263, 267–277, 280, 281–286, 292, 293, 295, 304, 306, 307, 308, 318, 326, 327, 330, 334, 335, 338, 339, 342, 343, 346
- Cyber security budgets, 208, 271, 272, 275
- Cyber terrorists, 126, 136, 137
- Cyber threat metrics, 158, 345
- Cyber vigilantes, 203, 204
- Cyber war, 20, 104, 153, 174, 175, 176, 217, 250, 264, 285, 286, 290, 313, 314, 319
- CyberCaliphate, 137
- Cybergeddon, 309, 310, 321, 329
- CyberPol, 319, 320, 330
- Cybersecurity Information Sharing Act, 188
- Cybertopia, 309, 315, 316, 318, 319, 321, 329
- D
- Damages provisions, 198
- Dark web, 1, 4, 56, 147, 148, 149, 152, 171, 202, 229, 316, 323, 339, 341, 347, 348
- Dark web prices, 148
- Dark web trading sites, 147
- Data controller, 191
- DDoS. *See* Distributed denial of service (DDoS)
- Deactivating fire suppression systems, 90
- Decision making, 86, 158, 159, 161, 209, 215, 279, 296
- Defending ourselves, 153
- Defense in depth, 223, 227, 228
- Denial of service attacks. *See* Distributed denial of service (DDoS)
- Designed for accidents, not malicious attacks, 88
- Detection, containment, and control, 220
- Directors and officers, 194, 239
- Disabling the safety system, 92
- Disaffected employees, 144
- Disk wiper, 46, 49, 142, 165, 170
- Distributed denial of service (DDoS), 14, 15, 30, 42, 55–62, 85, 108, 118, 120, 134, 135, 141, 165, 181, 181, 196, 202, 254, 288, 333, 339, 344, 353
- Domain Name System (DNS), 14, 135, 255
- Drucker, Peter, 154, 345
- Dyn, 14, 63, 99, 353
- Dynamic-link libraries, 114, 302

- E**
E-commerce, 6, 9, 14, 16, 62, 63, 64, 69, 125, 147, 254, 311, 313
Entering a secure facility, 89
Enterprise risk management (ERM), 193, 228, 261
Entropy, 323, 330
 password, 323
Equation Group, 104, 140, 143, 177, 337
Equifax, 30, 215, 225, 227, 228, 271, 272, 342, 345, 346
Errors as exploitable vulnerabilities, 104
Estimating population impacts, 112
EternalBlue, 44, 46, 177, 178, 187
 exploit, 177, 178, 187
European citizens' data rights, 190
Europol, 78, 130, 133, 171, 182, 202, 203, 306, 339, 340
Event tree, 166, 257
Events drive change, 231
Exfiltration, 1, 2, 7, 8, 12, 15, 16, 33, 34, 35, 37, 38, 40, 53, 64, 132, 137, 140, 148, 162, 165, 172, 174, 180, 196, 197, 213, 229, 245, 253, 254, 256, 257, 259
Expect the unexpected, 95
Expected loss, 22, 122, 192, 229, 273, 274, 275, 276
Exploits, 7, 14, 16, 51, 104, 105, 109, 121, 122, 134, 143, 174, 177, 217, 278, 282, 305
Exposure data, 252, 336
- F**
Failures of counterparties or suppliers, 33, 68, 162
FedEx, 45, 46, 47, 351
Financial consequences of a cyber attack, 225
Financial resilience, 225
Financial risk assessment, 226
Financial theft, 8, 63, 64, 140, 165, 239
FireEye, 172, 340, 343
Forensic investigation, 38, 218
Framework for risk assessment, 22, 23
Fraud, 4, 5, 6, 18, 34, 43, 49, 50, 63, 64, 65, 66, 67, 98, 132, 144, 169, 187, 189, 200, 213, 239, 349
Frequency-severity distribution, 22
FSB (Russian Federal Security Service), 173
Functioning black markets, 286
Future technology trends, 321
- G**
Gamification, 211, 352
Gaming and exercises, 211
GCHQ. *See* Government Communications Headquarters (GCHQ)

- General Data Protection
Regulation (GDPR), 190, 191,
245, 345
- Geneva Convention, 318, 331
- German steel mill,
cyber-physical attack on, 85
- Germany, 20, 45, 46, 53, 65,
132, 140, 221
- Getting the cyber risk future we
want, 328
- Getting users to install patches,
107
- Ghosts in the code, 28, 69,
103–123, 157, 315
- Global costs of cyber attacks,
25, 112
- Google, 14, 69, 72, 174, 202,
229, 281, 290, 327, 345, 347
- Gordon-Loeb model, 273, 275
- Government Communications
Headquarters (GCHQ), 140,
143, 204, 232, 324, 338, 351
- Growing consciousness of
cyber-physical interactions,
82
- H**
- Hacker hordes rise, 309
- Hacker motivations, 285
- Hackers, 1, 4, 14, 44, 46, 48,
52, 82, 87, 93, 96, 97, 98,
104, 106, 121, 125–128, 130,
134, 150, 151, 154, 156, 167,
168, 174, 179, 189, 205, 213,
214, 221, 229, 232, 255, 278,
281, 285, 286, 290, 292, 293,
298, 303, 305, 307, 310, 312,
315, 320, 323, 324, 338–344
- Hackers are rational game
players, 151
- ‘Hackerville’, 130, 352
- Hacking attacks on
cyber-physical systems, 83
- Hacking films, 82
- Hackonomics, 28, 126, 147,
150, 317
- Hacktivism, 62, 126, 134, 135,
254, 255
- Harvesting bugs, 174
- Hawking, Stephen. *See*
Quantum computing
- Heartbleed*, 229, 281
- Heartland Payment Systems,
66
- Hidden Lynx, 133, 350
- Hillis, Danny, 88, 102
- Home Depot, 39, 180, 197, 198
point of sale, 180
- How security enhancements
change the scenarios, 268
- How to cause damage remotely,
91
- How to subvert cyber-physical
systems, 88
- Human perception, 158
- Human vulnerability of staff,
144, 157
- Hurricane Irma, blamed by
Equifax, 215
- HVAC, 2, 3, 7
- Hypervisors, and cloud, 73, 230
- I**
- Identify, protect, detect,
respond, recover, 207
- ILOVEYOU*, 41, 42, 173

- Impact of security on cyber loss likelihood, 267
- Improving attribution, 288
- Improving the cyber profession, 218, 233
- Incident rate in advanced economies, 25
- Infrastructure as a service, 70
- Initial breach diagnosis, 219
- Insider theft and the cyber 'Big One', 177
- Insurance, 16, 24, 29, 30, 35, 36, 78, 129, 164, 170, 186, 192–196, 226, 227, 235–265, 275, 308, 333–338, 342, 345, 348, 349, 350, 353
- Insurance market segmentation, 251
- Intent and compromises, 92
- International cyber response and defence, 118
- Internet of things (IoT), 28, 62, 81, 95, 99, 167, 208, 224, 297, 302, 303, 315, 338, 342, 347, 350
- Interpol, 131, 202, 203, 317, 339
and Europol, 202
- IoT as an amplifier of risk, 167
- Issuing security patches, 106
- J**
- Jaschan, Sven. *See Sasser*
- JPMorgan Chase & Co., 67
- Jurisprudence and commerce, 183
- K**
- Kahneman, Daniel, 167
- Kaspersky Lab, 141, 151, 152, 211, 343
- Kerckhoff's principle, 96, 322
- Know your enemy, 28, 61, 85, 92, 125–152, 208, 285
- Knowing what could have occurred, 179
- Krebs, Brian, 4, 30, 343
- L**
- Law enforcement and cyber crime, 199
- Lazarus Group*, 65, 140, 178, 179, 305
- Leverett, Éireann, 78, 83, 102, 112, 123, 337, 344, 345
- Lifespan of software, 108
- Likelihood of future cyber losses, 22
- LinkedIn, password cracked, 323
- Lloyd's, 31, 101, 193, 254, 255, 256, 335, 344
- Logistical burden, 121, 148, 150, 310
- Logistical burden of cyber attacks, 148
- Long Term Viability Statement, 226
- Loss exceedance probability curve, 22
- Low conviction rates, 146, 200
- Low-hanging fruit, 279, 284

M

Maersk, 46, 47, 51
 attacked by *NotPetya*, 51
Making our devices safer, 100
Making smarter investment
 decisions, 270, 271
Malware overlap problem,
 303
Malware payloads, 49
Market for lemons, 287, 333
Marshall Plan, 331
Maskelyne, Nevil, 82, 328
Maupertuis, Pierre de, 284
McKinnon, Gary, 204, 205
Measurement, 22, 110, 114,
 153, 154, 155, 157, 299
Measurement and management,
 153
Measurement for better risk
 management, 157
Measurement to make
 improvements, 154
Measuring cyber attack severity,
 171
Measuring the threat for an
 organization, 162
MediaMark, 163, 164, 165,
 242, 243, 274
Melissa, 41, 42
Mercenary teams, 126, 133, 134
Microsoft patch, 44, 178
Minimizing intrusion dwell time,
 220
Misinformation, 210
Mitnick, Kevin, 168, 181,
 182, 345
MITRE Corporation, 109
Monitoring checklist, 155

Moody's Investors Service, 226,
 227, 234, 345
More powerful attack
 technologies being deployed,
 310
Mossack Fonseca, 136, 195,
 196, 332

N

Nation-state- and
 state-sponsored cyber teams,
 126, 139
National conflict strategies,
 287
National Institute of Standards
 and Technology, 108, 188,
 207, 273, 323, 346, 347
National Security Agency
 (NSA), 14, 44, 61, 105, 142,
 176, 187, 232, 278, 324
 and Edward Snowden, 176
National vulnerability agencies,
 118
NATO, 21, 307, 314, 348
Neiman Marcus, 6
Netsky, 41, 42, 49
Nortel, 30, 276
North Korea, 21, 140, 142, 153,
 178, 233, 276, 289, 305, 334
Not if or when, but how likely?,
 170
NotPetya, 13, 14, 24, 42, 46,
 47, 48, 51, 55, 105, 142, 249,
 338, 348, 349, 351
NSA. *See* National Security
 Agency (NSA)
Nudge theory, 107, 198
Nudging behavior, 212

O

- Operating compromised systems, 93
- Operational disruption causing loss of revenue, 9, 17, 25, 27, 343
- Overriding safety alerts, 89

P

- Password, 5, 35, 41, 46, 63, 120, 167, 168, 172, 202, 211, 322, 323, 324, 341, 350
- Patching latency, 51, 107, 275
- Path of least resistance, 158, 200, 225
- Pen test. *See* Penetration test
- Penalties for breach of GDPR, 191
- Penetration test, 82, 89, 106, 121, 132, 155, 223, 224, 230, 262, 285, 286, 312, 339, 341, 343
- Perception of threat, 158
- Phishing, 2, 8, 42, 65, 95, 128, 131, 132, 141, 144, 157, 162, 168, 171, 197, 210, 211, 221
- Platform as a service, 70
- PML scenarios, 252
- Point of sale (PoS), 1–7, 9, 47, 49, 50, 63, 64, 66, 132, 149, 180, 197, 198, 214, 338, 345, 349
 - at Home Depot, 198
 - at Target Corporation, 3
- Polymorphic virus, 306, 350
- Ponemon Institute, 30, 231, 234, 268, 269, 292, 294, 347

- Predictive power of company attributes, 262, 263
- Preparing for cyber conflict, 289
- Prioritizing mitigation against multiple scenarios, 97
- Probabilities of extreme cyber losses, 253
- Probable maximum loss (PML) scenarios, 252
- Professional liability, 195, 196
- Public key, in cryptography, 325, 326
- Putting bounties on their heads, 291

Q

- Quantifying vulnerability identification, 109
- Quantifying vulnerability severity, 110
- Quantum computing, 322, 326, 327, 328
- Quantum computing as a security risk, 327
- Quantum computing horizon, 326
- Quantum key distribution (QKD), 328

R

- Random number generation, 321
- Ransomware, 13, 14, 16, 30, 42, 43, 44, 46, 49, 50, 52–56, 128, 130, 142, 149, 165, 177, 178, 180, 204, 230, 253, 254, 306, 310, 335, 338, 339, 349, 351, 353

- Rapid adaptation to changing conditions, 209
- Rating and risk selection, 258
- Rational decisions, 24
- Reactive legal developments, 194
- Real-time crisis management, 208, 209
- Red-teaming, 225
- Regulation of cyber insurance, 192
- Regulations for finance, healthcare, and communications, 189
- Reimagining history, 178, 180, 352
- Rescator*, 1, 2, 3, 4, 6, 7
- Resilience, 29, 56, 78, 94, 96, 207–234, 315, 343, 344, 346, 353
- Resilience engineering, 212, 342, 353
- Resilient security solutions, 219
- Resilient software, 219
- Re-simulations of historical events, 229
- Rethinking the design time horizon, 297
- Risk audit, 199
- Risk capital, 243, 248, 250, 253, 258, 260
- Risk implications of the market for zero days, 283
- Risk Management Solutions, Inc., 24, 31, 336, 337, 348
- Risk of malware infection, 49
- Risk tolerance of the organization, 23, 273
- Risk-informed security enhancement, 273
- Risk-return trade-off, 224
- Role of rating agencies, 193
- RSA algorithm, 324, 36, 328
- Russia, 1, 4, 21, 45, 46, 47, 64, 65, 76, 129, 131, 132, 137, 139, 140–143, 173, 178, 179, 182, 222, 233, 276, 281, 288, 296, 298, 305, 307, 314, 346, 347, 349, 351
- Rustock, 291
- S**
- Sabotage, 33, 46, 53, 61, 83, 97, 100, 101, 141, 144, 221, 343
- Safety engineering, 212
- Safety management, 166, 212
- Salesforce, 70
- San Francisco municipal railway, 54
- Sasser*, 42, 290, 291
- Secure hash algorithm, 323
- Security as well as functionality, 296
- Security budget, 67, 157, 158, 208, 224, 231, 271–276, 292, 340
- Security economics, 29, 100, 154, 208, 267–294, 297, 334
- Security levels in connected devices, 99
- Security verification problem, 307
- Setting problems, 295
- ShadowBrokers*, 14, 44, 105, 143, 177, 178, 187, 278
- ShadowCrew*, 128, 129, 334

- Shaping portfolios by underwriting, 260
- Shodan, 112, 119, 123
- Shor, Peter, 327
- Shutting down the Ukrainian power grid, 84
- Silk Road. *See* Dark web
- Small companies, 201
- Smith, Rick. *See* Equifax
- Snowden, Edward, 38, 176, 181, 281, 342
- Social engineering, 128, 131, 148, 156, 157, 162, 168, 210, 211, 215, 220, 224, 275, 293, 296, 293, 303, 329, 338
- Societal cyber threats, 19
- Software as a service, 69
- Software dependency problem, 300
- Software development life cycle, 113, 115, 199, 220
- Software liability waiver, 316, 330
- Sony Pictures, 141
- Specializations in security solutions, 118
- Splinternet, 312, 313
- Spoofing the sensors, 86
- St Petersburg Paradox, 281
- Standardizing vulnerability identifiers, 109
- State-sponsored cyber teams, 126, 139, 140, 141, 143, 220, 222, 264, 289, 313, 314, 315, 330
- Stochastic models, 257, 258
- Strategies of cyber attack, 283
- Strategies of national cyber defence, 289
- Strategies of state-sponsored cyber teams, 289
- Stuxnet*, 42, 83, 86, 175, 176, 288, 353
- Subverting an insecure protocol, 87
- Sun Tzu, 168, 169, 185, 217, 285
- Supervisory control and data acquisition (SCADA) systems, 81
- Supply chain, 9, 68, 69, 115, 116, 117, 208, 209, 262, 302 due diligence, 115
- Sutton's Law, 200
- SWIFT, 13, 14, 63–66, 132, 141, 179, 232, 348, 350, 352 and *Lazarus Group*, 65
- T**
- Tail risk, 248–251, 253, 257, 258
- Target Corporation, 3, 4, 6, 7, 8, 34, 259
- Taxonomy of threat actors, 127
- Telematics assessments, 117
- Ten recommendations for our cyber future, 330
- Terrorists, 126, 136, 137, 158, 170, 225, 246
- Thaler and Sunstein's nudge theory, 198
- Theft of IP, 239

- Threat actors, 28, 60, 61, 64, 101, 121, 125, 127, 139, 145, 146, 147, 150, 208, 283, 309, 315, 337
- Threat actors and cyber risk, 145
- Threat analysis, 240
- Threat attributes, 159
- Threat matrices and attack trees, 160, 161
- Thyssenkrup, 221
- Triggering fake safety procedures, 89, 90
- Trump, Donald, 213, 214
- Trump Hotels, 213
- Turing, Alan, 295, 296, 321, 324
- Turing Test, 296
- Turning hackers legitimate, 286
- U
- Ukraine, 17, 21, 46, 47, 65, 84, 132, 339
power grid outage, 17
- Ultra-high intensity attacks, 59, 61, 62, 165
- Uncertainty Principle, 328
- Underwriting questionnaire, 242, 260, 262
- US cyber laws, 186
- US NIST National Vulnerability Database, 108
- Using compromises to take control, 92
- Using scenarios, 162
- V
- Value at risk (VaR), 228, 229
- Vandalism, 61, 144, 221, 277, 307
- Variation in risk over time, 98
- Verification, 4, 7, 63, 67, 243, 298, 307, 308, 318, 347
- Virus modification problem, 306
- Vulnerabilities, 8, 17, 20, 22, 28, 36, 63, 65, 68, 72, 73, 83, 85, 97, 98, 100, 104–111, 113, 114, 115, 116, 118–122, 127, 139, 148, 159, 174, 177, 186, 188, 199, 210, 211, 217, 231, 243, 244, 254, 262, 263, 275, 278–282, 284, 285, 286, 297, 301–304, 308, 311, 315, 316, 329, 330, 338, 345, 351
- Vulnerabilities Equities Process (VEP), 105, 177, 351
- Vulnerabilities impacting populations of companies, 111
- Vulnerabilities, exploits, and zero days, 104
- Vulnerability count problem, 302
- Vulnerability inheritance problem, 302, 303
- Vulnerability lifespan problem, 304
- Vulnerability management, 106, 111, 113
- W
- WannaCry*, 13, 14, 24, 42, 44, 45, 46, 55, 105, 142, 177, 178, 204, 230, 257, 335, 346, 348, 352

Ways things can go wrong, 167
Weakest link, 156, 168, 197,
208, 281, 311
Wells Fargo, 67, 340
Whistle-blowing, 38, 134, 144,
176
Wikileaks, 38, 66, 136
Worst-case scenarios, 92, 96

Y

Yahoo, 30, 172, 173, 180, 219,
271, 292, 340, 346

Z

Zero days, 14, 16, 104, 105,
121, 133, 134, 150, 174, 175,
176, 180, 220, 254, 256, 276,
277, 278, 281, 282, 283, 304,
333, 353
exploiting, 104
Zerodium, 282, 283
Zipf's law, 172, 257, 333

