## Index

### A
- Active Server Pages (ASPs) 183
- Adaptive Security Policy 326-327, 334-335, 340, 342
- Adaptive Real-time Alarm Management (AR-TAM) 174
- Agile Governance Model (AGM) 54
- Alert Coding (ALCOD) 174
- anonymity services -See web anonymizers.
- Application Programming Interfaces (APIs) 182
- attack lifecycle 286
- attribute verification classes 36, 46, 48
- automated auditing tools 390
- Availability management 321

### B
- Backup mechanism 324
- Bayesian filtering 120, 126, 253
- Behavioral Theory 327
- Binding Corporate Rules (BCRs) 181, 190-191
- Biometrics 341
- bisimulation 227-231
- Brute Force Attack 142, 157
- business-complementary partners 201
- Business Continuity Management System (BCMS) 226, 231
- Business Continuity Plan (BCP) 224, 231, 237
- Business Process Management Systems (BPMS) 387
- Business Process Visibility 402, 404
- business-to-business (B2B) relationships 197

### C
- CAG (Consensus Audit Guidelines) 80, 82
- capacity management 320
- Card-not-Present fraud losses 346, 352-353, 362-363, 365
- Cascading risks 204, 214
- Change management 321
- cloud agreement 187
- cloud-based computing 181-182
- cloud computing 57, 181-189, 191, 193-194, 232, 262
- cloud infrastructure 184-185
- cloud services 57, 185, 187-188
- Code Script Checking 251
- co-development partnerships 201
- Community cloud 185
- compliance failures 385
- Compliance Monitoring Verification 180
- Configuration management 321
- Context Aware Computing 332-333
- Context Aware Environment 333
- Continuous Authentication System 328, 343-344
- Control loops 226-227, 229, 242
- Corporate Governance (CG) 58
- corporate security 224, 269, 327, 408
- Counterfeit card fraud 363
- crackers 349
- credit card fraud 249, 346, 368
- credit fraud detection 346-347, 362
- cross site scripting 245
- cue-dependent forgetting 138, 155

### D
- Data Protection Authority (DPA) 191
- Dataveillance 172, 178, 180
- Deming cycle 223-224, 227-230
- Dictionary Attack 157
- diffusion of innovations theory 13-17, 27
- digital forensics 332
- digital identity 36
- digital signatures 256
- Direct-Control Cycle 56, 65
- discrete-event systems theory (DES) 227
Distributed Denial-of-Service (DDoS) 332
DNS Cache poisoning 247
Domain Keys (DK) 256
domain name spoofing 245

E

e3value model 200, 208
e-business 347
e-business fraud 346, 363
EC2 (Elastic Compute Cloud) 182
e-commerce 347
e-fraudster 347
Electronic Learning Module Systems (ELMS) 302, 306
electronic signatures 17
E-Mail Authentication 245, 256, 259
Enterprise Governance (EG) 58
Enterprise Information Security Policies 67, 72-73
Enterprise Risk Management 65-66, 219, 385, 387
ERP (Enterprise Resource Planning) 211
e-transaction 347
EU standard contract clauses 181, 191
Extended Enterprise 195-197, 200-204, 206-208, 210, 213-215, 217-220
External Insiders 195-208, 210-215, 221

F

Facebook Generation 405, 409-411, 418-419
Federated Identity Management (FIM) 24, 38
firewalls 256
Fuzzy set theory 177

G

Generation F - See Facebook Generation
Generation of Security Management Patterns (GSMP) 90-91
Generation Y - See Facebook Generation
Greenfield deployment 318

H

Herzberg’s Two Factor Theory of Motivation 84
Human Resources Management System (HRMS) 410
Hybrid cloud 185

I

Identified Internet Mail (IIM) 256
identity assurance 34
Identity Assurance Frameworks 39
identity fraud 36, 245, 350
Identity Management (IdM) 24
Identity Management Systems (IMS) 24
identity theft 160, 181, 186, 245-249, 257-259, 368
Incident management 321
InCommon Identity Assurance Assessment Framework 39
Independent Back Channel 46
independent identity management systems 37
infinite alphabet password (IAP) model 141
Information Governance 57, 182, 194
Information personnel training 322
information risk management 317, 319, 323
Information security
guidelines 69-70
policies 69-70
procedures 69-70
standards 69-70
Information Security 54, 56
information security awareness 3, 7-8, 11, 87, 276, 280, 313, 412
Information security controlling 274, 276-278
information security controls 69, 270
information security culture 1, 297-298
Information Security Disclosure 405, 419-420
Information Security Documents Framework 70-71
Information Security Forum (ISF) 55, 62
Information Security Management (ISM) 55
Information Security Management Systems (ISMSs) 90-91
Information Security Practices 3, 296-297, 299, 310, 315, 409, 411
Information Technology Security Assessment 116
informatization 316, 318, 324
Infrastructure as a Service (IaaS) 185
infrastructure vulnerabilities 329
In-Person Proofing 41, 44, 46
Installed base 318
interactive innovation 16
Internal Control Point 389-390, 397-398, 404
International Organization for Standardization (ISO) 55, 77
International Safe Harbor Certification 190
Internet banking (IB) 349
Intrusion Detection Systems 328
Issuer-Controlled 46
IT Governance (ITG) 54
ITIL (IT Infrastructure Library) 320
IT service continuity management 321
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITSM (Information Technology Service Management System) 223-224</td>
</tr>
</tbody>
</table>

**K**
- Karma System 129-130
- killer apps 182

**L**
- Legacy deployment 318
- levels of assurance (LoA) 36, 48, 52
- Low and Low Attack 157

**M**
- Machine Learning 118, 124-127, 132, 135-136, 175, 258-259
- malware 355
- Methodology for Security Management and Maturity in Small and Medium-size Enterprises (MSM2-SME) 90
- Ministry of Defence (MoD) 413, 420
- Musical passwords 139-140, 142, 145-146, 149, 151-152
- Musipass 137-138, 140, 142-153

**N**
- Naïve Bayesian filters 253
- National Institute of Standards and Technology (NIST) 40, 74, 77, 279
- natural disasters 324
- neuro-fuzzy systems 342
- NIST 800-63 40
- noncompliant event (NCE) 175

**O**
- Observe, Orient, Decide, Act (OODA) 171
- OMB M-04-04 40
- Online Credit Fraud 350
- Online Fraud Prevention 363
- OpenID 24, 38, 45, 50-51, 156
- open identity management systems 34-35, 37, 52
- Operant conditioning 327
- organizational culture 1-2, 4-7, 11, 84, 296, 298, 304-305, 309-313, 315
  - differentiation perspective 4
  - fragmentation perspective 4
  - integration perspective 4
- Organizational Security Monitoring Design 328

**P**
- parsing 253
- Password Space 140, 157
- PDCA cycle 227-229, 231, 242, 264
- peer-to-peer (P2P) networks 249
- Personal Data Protection Act 164
- Personality rights 329-330
- pharming 160
- phishing 249
- phishing attacks 245, 247, 251, 254, 256-259
- Phishing Scams 249, 252-253, 256-257
- phronesis 8
- physical security 323
- Plan-Do-Check-Act (PDCA) 227
- Platform as a Service (PaaS) 185
- Pretty Good Privacy (PGP) 20
- preventive innovation 18
- privacy technology 23-24
- Private cloud 182, 185
- Problem management 321
- Protection of Classified Information Act 164
- Public cloud 185
- public key cryptography 19, 255-256

**R**
- Reusable Pattern for Security Management (RPSM) 90-91
- role repertory grid 285
- Routine information environment maintenance 322

**S**
- safe harbor certification 190
- Safety information system 159
- Secondary Monitoring 174, 180
- Secure Socket Layer (SSL) 251
- security awareness 3
- Security Culture 1-12, 104-105, 110-112, 115-116, 296-300, 310-313, 315
- security documents 69
- security management system (SMS) 99
- Security Metrics 116, 273, 276, 280-281
- security testing 166, 323
- Security Training and Awareness 315
- Self-Aware Pervasive System 334

Organization for Economic Co-operation and Development (OECD) 279, 297
Index

Sender ID Framework (SIDF) 255
Sender Policy Framework (SPF) 245, 252, 254-255, 260
service desk 321
Service level management 320
Signal Detection Theory 172, 178
single-sign-on (SSO) 38, 157
Skinner Theory 327
Small and Medium-size Enterprises (SMEs) 90-91
Social engineering 73, 160-161, 247
Social networking sites (SNSs) 117
Social spamming 125
social tagging system 120
socio-ethical controls 3, 12
Software as Service (SaaS) 182
Spam Assassin 253
Spear Phishing 249, 258, 260
Spyware 355
standard contractual clauses (SCCs) 191
Standard of Good Practice for Information Security (SOGP) 55, 62
statistical phishing filters 252
Structural Clustering Algorithm for Networks (SCAN) 123
Stuxnet worm 68, 73, 86-87
Supervisory Control and Data Acquisition (SCADA) 369
surveillance communities of practice 170-171
Surveillance Thresholds 180
susceptive e-mails 245
suspected non-compliant events (SNCEs) 174
Sustainable information security 262, 267, 272, 276-278
system lifecycle 283, 286-287
Target Function 224, 239-242, 244, 325
TCSEC (Trusted Computer System Evaluation Criteria) 165
technology acceptance model 14, 17
Threats Management 163
Tokenization 253
total quality management (TQM) 299
trace-dependent forgetting 138
trading partners 200
transborder transfer 188
Trojan Horses 160, 247
trusted authentication 332
two-factor authentication 255
Uberveillance 180
UK Office of the e-Envoy 40
Unmanaged Business Processes 385, 404
URL obfuscation 245, 250-251
user behavior analysis 326-327, 332, 334-336, 339-340, 342-343
user-centric identity management 37
verification classes 46
Virtual Banking - See Internet Banking.
Virtual Private Networks (VPNs) 332
web anonymizers 21
WHOIS query 253
Wikileaks 407