

Index

Symbols

32-bit viruses 53

802.1x protocol 239

9/11 (September 11, 2001, terrorist attack)
154

A

AAA (authentication, authorization, and
accounting) server 354

Abstract State Machine Language (ASML)
226

access control list (ACL) 90, 99, 210, 334

access management 373

access point (AP) 244

accounting FU (AFU) 102

ACL (access control list) 90, 99, 210, 334

action planning 85

Advanced Encryption Standard (AES) 238

AEGIS (appropriate and effective guidance
in information) 220

AES (Advanced Encryption Standard) 238

Akamai 26, 30

Global Network System Policy

Handbook 36

Web portal implementation 30

alteration 236

Amazon.com 135

anomaly detection 258

anti-debugging 55

anti-emulation 55

anti-fraud 76

Anti-honeypot Alliance 282

Anti-Spyware 51

antivirus 140

antivirus (AV) 58, 213

detection 52

software 22, 43

AP (access point) 244

application programming interface (API)
365

API (application programming interface)
365

appropriate and effective guidance in
information (AEGIS) 220

AS (authentication server) 353, 355

ASML (Abstract State Machine Language)
226

asset identification 85

Association for Payment Clearing Services
147

assurance 182

asymmetric (public) key 99

auditing 98

authentication, authorization, and accounting (AAA) server 354
 authentication complexity-based taxonomy 347
 authentication middleware 364
 authentication protocols 352
 authentication quality-based taxonomy 346
 authentication scope-based taxonomy 348
 authentication server (AS) 353, 355
 availability 235
 awareness 132

B

B2B (business-to-business) 80, 102
 B2C (business-to-consumer) 102, 131
 B2C (business-to-customer) 81
 backdoor, *see also remote-access Trojan* 56
 Baseline Protection Manual 115
 BGP (border gateway protocol) 209
 biometric 351
 Blaster 22
 border gateway protocol (BGP) 209
 British Standard (BS) 115
 Bugbear worm 135
 business-to-business (B2B) 80, 102
 business-to-consumer (B2C) 102, 132
 business-to-customer (B2C) 81

C

CAIN (confidentiality, authentication, integrity, and non-repudiation) 170
 CAs (certificate authorities) 361
 capability maturity models (CMMs) 175
 CASE 230
 case study, Singapore-based MNC company 88
 central redundant architecture (CRA) 157
 centralization 19
 IS 19
 IT security management 21
 certificate authorities (CAs) 361
 Certified Information Systems Auditor (CISA) 63
 CEO (chief executive officer) 182
 challenge-response protocol 353

Chartered Institute of Management Accountants (CIMA) 3
 check-summing (integrity checking) 52
 chief executive officer (CEO) 182
 chief information officer (CIO) 26, 182
 chief security officer (CSO) 182, 293
 CIMA (Chartered Institute of Management Accountants) 3
 CIO (chief information officer) 26, 182
 CISA (Certified Information Systems Auditor) 63
 CMMs (capability maturity models) 175
 COBIT (Control Objectives for Information and related Technology) 18, 64, 113
 CommerceNet 134
 commercial off-the-shelf (COTS) 192
 Committee of Sponsoring Organizations of the Treadway Commission (COSO) 64
 Common Criteria 115, 173
 Common Criteria (CC) 187
 Common Criteria (CC)) 182
 computer crime 312
 computer criminals 312
 Computer forensics 313
 Computer Security Institute (CSI) 27
 Computer Trespasser Exception 274
 computer-aided software engineering (CASE) 230
 confidentiality 235
 confidentiality, authentication, integrity, and non-repudiation (CAIN) 170
 configuration management
 personnel management 171
 consent clause 274
 consumers 131
 control FU (CFU) 102
 Control Objectives for Information and related Technology (COBIT) 18, 64, 113
 corporate governance 63
 COTS (commercial off-the-shelf) 192
 COSO (Committee of Sponsoring Organizations of the Treadway Commission (COSO) 64
 CPU 328
 CRA (central redundant architecture) 157

cryptography 99, 288
 CSO (chief security officer) 182, 293
 curador 136
 cyber crimes 312

D

DAC (discretionary access control), 99, 303
 data capture 277
 data control 276
 Data Encryption Standard (DES) 100, 140
 data hiding 315
 data warehouses (DWs) 295, 296
 database management systems (DBMS) 296
 DBMS (database management systems) 296
 decentralized IS 20
 decryption 315
 heuristic-based 55
 defense-in-depth 237
 demilitarized zone (DMZ) 197
 denial-of-service (DoS) 44, 104, 131, 135, 197, 213, 216, 240, 256
 Department of Defense (DOD) 183
 Department of Trade & Industry 134
 DES (Data Encryption Standard) 100, 140
 detection 118, 254
 DHCP (dynamic host configuration protocol) 363
 digital forensics 311, 312
 Digital Signature Standard (DSS) 140
 directory services 373
 disaster recovery 152
 discretionary access control (DAC), 99, 303
 disruption 236
 distributed partially redundant architecture (DPRA) 159
 distributed systems 156
 district sales managers (DSM) 30
 DMZ (demilitarized zone) 197
 DNS (domain name service) 199, 212
 Split DNS (also called split name space) 212
 DOD (Department of Defense) 183
 domain name service (DNS) 199, 212

DoS (denial-of-service) 44, 104, 131, 135, 197, 213, 216, 240, 256
 DPRA (distributed partially redundant architecture) 159
 DSD (dynamic separation of duties) 127
 DSM (district sales managers) 30
 DSS (Digital Signature Standard) 140
 DSV (dynamic signature verification) 352
 DWs (data warehouses) 295, 296
 dynamic host configuration protocol (DHCP) 363
 dynamic separation of duties (DSD) 127
 dynamic signature verification (DSV) 352

E

e-business (electronic business) 1, 6, 80, 81
 e-commerce 132
 threats 134
 e-enterprise 95
 e-enterprise security profile (ESP) 101
 EAL (evaluation assurance levels) 173, 183
 EAP (extensible authentication protocols) 239
 eavesdropping 236
 EI (enterprise integration) 95
 EI methodology (EIM) 97
 electronic business (e-business) 1, 6, 80, 81
 encrypted virus, 54
 encryption 140, 236, 315
 Enron® 2
 enterprise
 deployment 43
 integration (EI) 95
 resource planning (ERP) 6, 19
 entry point obscuring (EPO) 53
 ERP (enterprise resource planning) 6, 19
 ESP (e-enterprise security profile) 101
 European Union (EU) 296
 evaluation assurance levels (EAL) 173, 183
 extensible authentication protocols (EAPs) 239
 Extensible Markup Language (XML) 345

F

Federal Information Processing Standard (FIPS) 192

federated identity 374
 FieldWeb 26
 FIPS (Federal Information Processing Standard) 192
 firewalls 43, 211, 266
 flexible modeling framework (FMF) 220
 forensics 313
 Fourth Amendment 272
 FU capability excess (FUPX) 105
 FU security capabilities (FUSC) 101
 functional unit (FU) 97
 FUPX (FU capability excess) 105
 FUSC (FU security capabilities) 101

G

generic routing encapsulation (GRE)
 tunnels 280
 German IT Baseline Protection Manual 115
 GINA (graphical identification and authentication) 331
 Global System for Mobile Communications (GSM) 355
 GMITS (Guidelines on the Management for IT Security) 115
 graphical identification and authentication (GINA) 331
 graphical user interface (GUI) 291
 GRE (generic routing encapsulation)
 tunnels 280
 GUI (graphical user interface) 291
 Guidelines on the Management for IT Security (GMITS) 115

H

hacker 42, 134, 267, 312
 hash functions 140
 heuristics 55
 Honeyd 269
 Honeynet Project 276
 honeynet tuning 279
 honeynet 267, 268
 honeypot 209, 268
 honeywall 277
 host 277
 host-based intrusion detection 256

I

IA (information assurance) 192
 IATF (Information Assurance Technical Forum) 115
 ICMP (Internet control message protocol) 263, 269
 ICT (information and communications technology) 2
 ICT governance 5
 identity management (IdM) 373
 strategic focus 377
 IdC (Internet data center) 88
 IDS (intrusion detection system)
 90, 209, 211, 254, 266, 339
 knowledge-based 258
 network-based intrusion 257
 performance 260
 IEEE 18
 IEEE 802.11i standard 238
 IFAC (International Federation of Accountants) 3
 IFCC (Internet Fraud Complaint Center) 133
 IFIP (International Federation for Information Processing) 217
 IMAP (Internet message access protocol) 47
 IM (instant messaging) 47
 information and communications technology (ICT) 2
 information assurance (IA) 192
 Information Assurance Technical Forum (IATF) 115
 information protection network (IPN) 197
 information security (IS) 25, 43, 168
 centralized 19
 decentralized 20
 governance (ISG) 5
 policy 43
 information superhighway 43
 information system (IS) 19, 30, 71, 151, 298
 information systems architecture 158
 information technology (IT)
 1, 63, 96, 112, 151, *see also IT (information technology)*
 Information Technology Security Evalua-

tion Criteria (ITSEC) 188
 instant messaging (IM) 47
 integrity 235
 integrity checking (check-summing) 52
 interactive network (IN) 30
 Interception 236
 International Federation for Information Processing (IFIP) 217
 International Federation of Accountants (IFAC) 3
 International Standards Organization (ISO) 188
 Internet connections 205
 Internet control message protocol (ICMP) 263, 269
 Internet data center (iDC) 88
 Internet Engineering Task Force 140
 Internet Fraud Complaint Center (IFCC) 133
 Internet message access protocol (IMAP) 47
 Internet protocol security (IPSec) 208
 Internetwork packet exchange (IPX) 358
 intra-organizational commerce 81
 Intranet servers 48
 intrusion detection 100, 253
 intrusion detection system (IDS), *see also IDS (intrusion detection system)* 90, 209, 211, 254, 266, 339
 intrusion prevention system (IPS) 209, 212, 240
 IP packets 56
 IPN (information protection network) 197
 IPSec (Internet protocol security) 208
 IPX (Internetwork packet exchange) 358
 IS *see information security (IS), or information system (IS)*
 ISG (information security governance) 5
 ISO (International Standards Organization) 188
 ISO Standard 15408, *see also Common Criteria (CC)* 189
 ISO/IEC 17799 174
 IT (information technology) 1, 63, 96, 112, 151
 governance 2, 16, 18, 68
 redundancy 151

IT Governance Institute 18
 IT Governance Institute (ITGI®) 4, 18
 ITGI® (IT Governance Institute) 4, 18
 ITSEC (Information Technology Security Evaluation Criteria) 188

K

Kerberos 345
 keystroke verification 352
 knowledge-based intrusion detection systems 258

L

LAN (local area network) 344
 LAN manager (LM) 331
 LDAP (lightweight directory access protocol) server 330
 LEAP (lightweight extensible authentication protocol) 239
 least significant bit (LSB) 289
 legacy systems 173
 lightweight directory access protocol (LDAP) server 330
 lightweight extensible authentication protocol (LEAP) 239
 Linux security modules (LSM) 335
 LM (LAN manager) 331
 local area network (LAN) 344
 LSB (least significant bit) 289
 LSM (Linux security modules) 335

M

MAC (mandatory access control) 99, 127, 235, 303, 345
 MAC (media access control) 239
 MAC (message authentication code) 141
 Mafiaboy 135
 MailFrontier 133
 malicious software, *see malware*
 malware 23, 42, 135, 256
 history 44
 impact 43
 mechanics 52
 management process 81

- mandatory access control (MAC) 99, 127, 235, 303, 345
- Massachusetts Institute of Technology (MIT) 353
- MCHAP (Microsoft CHAP) 350
- MD5 (Message Digest 5) 140
- MDSCL (multidimensional security constraint language) 299
- MDX (multidimensional expressions) 299
- media access control (MAC) 239
- merchants 132
- message authentication codes (MACs) 141
- Message Digest 5 (MD5) 140
- message integrity code (MIC) 239
- Microsoft CHAP (MCHAP) 350
- middleware 364
- misuse detection, *see also knowledge-based intrusion detection system* 258
- MIT (Massachusetts Institute of Technology) 353
- MNC (multi-national corporations) 93
- MOMT (multilevel object-modeling technique) 297
- multi-national corporations (MNC) 93
- multidimensional (MD) models 296
- multidimensional expressions (MDX) 299
- multidimensional security constraint language (MDSL) 299
- multilevel object-modeling technique (MOMT) 297
- multiple-factor authentication 347
- MySQL 357
- N**
- NAS (network access server) 357
- NAS (network-attached storage) 48
- NAT (network address translation) 209, 210
- National Cyber Security Partnership (NCSP) 6
- National Information Assurance Partnership (NIAP) 192
- National Security Agency (NSA) 185
- National Security Telecommunications and Information Systems Security Policy (NSTISSP) 192
- NCSP (National Cyber Security Partnership) 6
- network 277
- network access server (NAS) 357
- network address translation (NAT) 209, 210
- network deception 267
- network file system (NFS) 356
- network forensics 313
- network information system (NIS) 356
- network interface cards (NICs) 244
- network-attached storage (NAS) 48
- networking 234
- NFS (network file system) 356
- NIAP (National Information Assurance Partnership) 192
- NICs (network interface cards) 244
- NIS (network information system) 356
- NSA (National Security Agency) 185
- NSTISSP (National Security Telecommunications and Information Systems Security Policy) 192
- O**
- Object-Constraint Language (OCL) 300
- object-modeling technique (OMT) 297
- OCL (Object-Constraint Language) 300
- OECD (Organisation for Economic Co-operation and Development) 3, 63
- OLAP (online analytical processing) 299
- OMT (object-modeling technique) 297
- one-time passwords 350
- online analytical processing (OLAP) 299
- open shortest path first (OSPF) 209
- operating system (OS) 214
- operations FU (OFU) 102
- Oracle 357
- Oracle Label Security (OLS10g) 295
- Orange Book 192
- Orange Book rating, 183
- Organisation for Economic Co-operation and Development (OECD) 3, 63
- OS (operating system) 214
- OSPF (open shortest path first) 209

P

- P2P (peer-to-peer) 47
- PANA (protocol for carrying authentication for network access) 352
- password authentication protocol (PAP), 350
- passwords 239
- patch deployment 49, 50
- patch management 50
- Patriot Act 274
- PaymentOne 133
- PayPal service 137
- PBT (property-based tester) 220
- PCAOB (Public Company Accounting Oversight Board) 71
- PE (portable extension) 52
- PEAP (protected extensible authentication protocol) 239
- Pen Trap Act 272
- performance measurement 3
- perimeter protection 100
- pharming 42
- phishing 42
- physical decentralization 150
- physical intrusion 255
- physical security 235
- pluggable authentication module (PAM) 332, 365
- policy 17, 21
- polymorphic viruses
- port scan attacks 256
- portable extension (PE) 52
- prevention 254
- privacy regulations 243
- private key 351
- procedure 21, 22
- property-based tester (PBT) 220
- protected extensible authentication protocol (PEAP) 239
- protection 117
- protection profile (PP) 189
- protocol for carrying authentication for network access (PANA) 352
- Provider Protection Clause 273
- provisioning 377
- proxy server 349

- Public Company Accounting Oversight Board (PCAOB) 71

- public (asymmetric) key 99
 - cryptography 351
- public key infrastructure (PKI) 209, 239, 374
- public zone 206

R

- radio frequency (RF) 344
- RADIUS (radius authentication dial in user service) 355
- random intrusion 256
- RAS (remote access server) 48
- rational unified process (RUP) 221
- reaction 119
- reliability 155
- remote access server (RAS) 48
- remote-access Trojan 56
- resource utilisation 3
- response 254
- restricted zone 206
- retrovirus 55
- return on investment (ROI) 380
- reverse proxy 212
- RF (radio frequency) 344
- risk
 - assessment 49, 66, 85
 - management 3, 10, 12, 235, 246

- Rivest-Shamir-Adleman (RSA) 100, 140
- ROI (return on investment) 380
- role-based access control (RBAC) 99, 127, 221, 335
- root security policy (RSP) 29
- routers 210
- RSP (root security policy) 29
- RUP (rational unified process) 221

S

- S-Tools 291
- S/MIME (secure multi-purpose Internet mail extensions) 361
- SA (Standards Australia) 4
- safeguards 132
- SAM (security account manager) 331

- SAN (storage area network) 48
- SANS (Systems Administration and Networking Security Institute) 27
- Sarbanes-Oxley (SOX) Act of 2002 2, 62
- SATs (security assessment tools) 220
- SMB (server message block) 47
- Sebek 278
- SEC (Security and Exchange Commission) 70
- secure electronic transaction (SET) 142, 361
- Secure Hash Algorithm (SHA) 140
- secure multi-purpose Internet mail extensions (S/MIME) 361
- secure remote password protocol (SRP) 352
- secure repository 373
- secure repository, *see provisioning* 373
- Secure Shell (SSH) 209, 357
- secure socket layer (SSL) 209
- secure socket layer/transport layer security (SSL/TLS) 361
- security 6, 81, 155
- security account manager (SAM) 331
- Security and Exchange Commission (SEC) 70
- security assessment tools (SATs) 220
- security
 - control 80, 81
 - domains 95, 187
 - engineering 216, 218
 - identifier (SID) 331
 - labels 302
 - management 95
 - management methodology (SMM) 97, 105
 - metrics 95
 - policy 30
 - profile 95
 - profile deficit (SPD) 105
 - risks 352
 - target (ST) 189, 190
- Security Operations Committee (SOC) 36
- Security-enhanced Linux (SELinux) 335
- September 11, 2001, terrorist attack (9/11) 154
- serial line Internet protocol (SLIP) 358
- server message block (SMB) 47
- service set identifier (SSID) 237
- SET (secure electronic transaction) 142, 361
- Shibboleth 345
- SID (security identifier) 331
- SIM (Society for Information Management) 156
- SIM (subscriber identity module) 351
- simple mail transfer protocol (SMTP) 47
- simple network management protocol (SNMP) 90, 242
- simple object access protocol (SOAP) 345
- simple policy control project (SPOCP) 345
- single sign-on (SSO) 99, 333, 374
- single-factor authentication 347
- SLIP (serial line Internet) 358
- small and medium enterprises (SMEs) 112
- SMM (security management methodology) 97, 105
- SMTP (simple mail transfer protocol) 47
- SNMP (simple network management protocol) 90, 242
- SOAP (simple object access protocol) 345
- Sobig.F worms 22
- SOC (Security Operations Committee) 36
- Society for Information Management (SIM) 156
- software
 - design 222
 - development management 171
 - engineering 216
 - forensics 313
 - metrics 96
 - process models 217
- Software Security Assessment Instrument (SSAI) 220
- software security checklist (SSC) 220
- software security engineering 216
- SpamMimic 290
- spamming 42
- SPD (security profile deficit) 105
- Split DNS (also called split name space) 212
- SPOCP (simple policy control project) 345
- spoofing 42, 256

- spyware 42
- SRP (secure remote password protocol) 352
- SSAI (Software Security Assessment Instrument) 220
- SSC (software security checklist) 220
- SSD (static separation of duties) 127
- SSE-CMM (system security engineering capability maturity model) 175, 220
- SSH (Secure Shell) 209, 357
- SSID (service set identifier) 237
- SSL handshake protocol 140
- SSL record protocol 140
- SSL/TLS (secure socket layer/transport layer security) 361
- stakeholders 121, 217
- standards 81
- Standards Australia (SA) 4
- State Transition Analysis Technique Language (STATL) 226
- static separation of duties (SSD) 127
- statistical one-bit lightweight authentication (SOLA) 352
- STATL (State Transition Analysis Technique Language) 226
- steganalysis 291
- steganography 287, 288, 315
- storage area network (SAN) 48
- subscriber identity module (SIM) 351
- survivability 155
- Symantec 134
- symmetric (private) key 99
- system
 - analysis 169
 - engineering 168, 222
 - protection 100
- system security engineering capability maturity model (SSE-CMM) 175, 220
- Systems Administration and Networking Security Institute (SANS) 27

T

- TACACS (Terminal Access Controller Access Control System) 358
- TACACS+ 359
- targeted intrusion 255

- TCB (trusted computing base) 186
- TCP (transmission control protocol) 269
- TCP/IP (transmission control protocol/internet protocol) 197
- TCSEC (Trusted Computer System Evaluation Criteria) 183
- Telnet 90
- temporal RBAC (TRBAC) 102
- temporary key integrity protocol (TKIP) 238
- Terminal Access Controller Access Control System (TACACS) 358
- TGS (ticket-granting server) 353
- The Computer Fraud and Abuse Act 274
- The Pen Trap Act 274
- the secure sockets layer (SSL) protocol 140
- The Wiretap Act 273
- threat assessment 117
- threats 132
- ticket-granting server (TGS) 353
- TKIP (temporary key integrity protocol) 238
- TLS (transport layer security) 140, 238
- transmission control protocol (TCP) 269
- transmission control protocol/internet protocol (TCP/IP) 197
- transport layer security (TLS) 140, 238
- TRBAC (temporal RBAC) 102
- trouble ticketing system (TTS) 91
- TRUSTe 133
- Trusted Computer System Evaluation Criteria (TCSEC) 183
- trusted computing base (TCB) 186
- trusted products 182
- TTS (trouble ticketing system) 91

U

- UDP (user datagram protocol) 268
- UDP/IP (user datagram protocol/internet protocol) 356
- Unified Modeling Language (UML) 219, 295
- universal serial bus (USB) token chip 350
- user datagram protocol (UDP) 268
- user datagram protocol/internet protocol (UDP/IP) 356

V

- verification management 171
- VeriSign 142, 145
- virtual local area network (VLAN) 198, 280
- virtual machines 280
- virtual personal network (VPN) 238
- virtual private network (VPN) 48, 88, 201, 209, 357, 375
- virus
 - 32-bit viruses 53
 - encrypted 54
 - detection database 58
 - lifecycle 46
 - polymorphic 54
 - encrypted 54
 - retrovirus 55
- vulnerability management 171

W

- WAN (wide area network) 206
- war-driving 236
- Web cache 212
- Web site defacement 135
- Web-based portal 26
- WEP (wired equivalent privacy) 238, 363
- Wi-Fi Protected Access (WPA) 363
- wide area network (WAN) 206
- wired equivalent privacy (WEP) 238, 363
- wireless
 - access points 235
 - LANs (WLANs) 344
 - networking 234
 - security 235
 - transmissions 236
- Wiretap Act 272
- WLANs (wireless LANs) 34
- World Trade Center (WTC) 152
- WPA (Wi-Fi Protected Access) 363
- WPA2 363
- WTC (World Trade Center) 152

X

- XTACACS 358
- XML (Extensible Markup Language) 345

Single Journal Articles and Case Studies Are Now Right at Your Fingertips!

Purchase any single journal article or
teaching case for only \$18.00!

Idea Group Publishing offers an extensive collection of research articles and teaching cases that are available for electronic purchase by visiting www.idea-group.com/articles. You will find over ~~275~~ **980** journal articles and over ~~275~~ case studies from over 20 journals available for only \$18.00. The website also offers a new capability of searching journal articles and case studies by category. To take advantage of this new feature, please use the link above to search within these available categories:

- ◆ Business Process Reengineering
- ◆ Distance Learning
- ◆ Emerging and Innovative Technologies
- ◆ Healthcare
- ◆ Information Resource Management
- ◆ IS/IT Planning
- ◆ IT Management
- ◆ Organization Politics and Culture
- ◆ Systems Planning
- ◆ Telecommunication and Networking
- ◆ Client Server Technology
- ◆ Data and Database Management
- ◆ E-commerce
- ◆ End User Computing
- ◆ Human Side of IT
- ◆ Internet-Based Technologies
- ◆ IT Education
- ◆ Knowledge Management
- ◆ Software Engineering Tools
- ◆ Decision Support Systems
- ◆ Virtual Offices
- ◆ Strategic Information Systems
Design, Implementation

You can now view the table of contents for each journal so it is easier to locate and purchase one specific article from the journal of your choice.

Case studies are also available through XanEdu, to start building your perfect coursepack, please visit www.xanedu.com.

For more information, contact cust@idea-group.com or 717-533-8845 ext. 10.

———— **www.idea-group.com** ————

 **IDEA GROUP INC.**



Experience the latest full-text research in the fields
of Information Science, Technology & Management

InfoSci-Online

InfoSci-Online is available to libraries to help keep students, faculty and researchers up-to-date with the latest research in the ever-growing field of information science, technology, and management.

The InfoSci-Online collection includes:

- Scholarly and scientific book chapters
- Peer-reviewed journal articles
- Comprehensive teaching cases
- Conference proceeding papers
- All entries have abstracts and citation information
- The full text of every entry is downloadable in .pdf format

Some topics covered:

- Business Management
- Computer Science
- Education Technologies
- Electronic Commerce
- Environmental IS
- Healthcare Information Systems
- Information Systems
- Library Science
- Multimedia Information Systems
- Public Information Systems
- Social Science and Technologies

**InfoSci-Online
features:**

- Easy-to-use
- 6,000+ full-text entries
- Aggregated
- Multi-user access

"...The theoretical bent of many of the titles covered, and the ease of adding chapters to reading lists, makes it particularly good for institutions with strong information science curricula."

*— Issues in Science and
Technology Librarianship*



To receive your free 30-day trial access subscription contact:

Andrew Bundy

Email: abundy@idea-group.com • Phone: 717/533-8845 x29

Web Address: www.infosci-online.com

InfoSci-Online

Full Text • Cutting Edge • Easy Access

A PRODUCT OF  **IDEA GROUP INC.**

Publishers of Idea Group Publishing, Information Science Publishing, CyberTech Publishing, and IRM Press

infosci-online.com