INDEX

Advanced Encryption Standards (AES), 47–48
Adware, 100
AlgoSec, 100–101
American Institute of Certified Public Accountants (AICPA), 25–26
Antispam, 106
Antispyware, 106
Antivirus software, 99–102, 106
Apple's iOS, 38–39
Application programming interface (API), 61
Application software, 38–39
Argus, 100
Artificial intelligence (AI), 42, 44, 101, 141
  AI-based data monitoring, 108
  technologies, 32–33
Asset ownership for cryptocurrencies, 110–111
AxCrypt, 100

Bachelor of science (BS), 130
Big Data Analytics, 111–112
Bitdefender Antivirus, 100
Blockchain, 109–111
  encryption process, 47
  technology, 46–47
Border routers, 103, 106
BSA, 107
Burp Suite, 100
Business, 144–145
Business Email Compromise (BEC), 10
Business management, 144–145

Capture-the-flag (CTF), 133–134
CAQ, 25–26
Case-based scenario, 34–35
Center for Internet Security (CIS), 25–26
Center for Strategic and International Studies (CSIS), 14
Chaos engineering, 57–59

Chaos Monkey, 58
Classical computers, 48–49
Cloud computing technology, 51–52
Cloud-enabled data trusts, 109
COBIT framework, 26–27
Cognitive psychology, 141
Community colleges, 129
Competencies, 67
CompTIA Security+, 126–127
Computer and network security, 41
Computer hardware, 38
Computer networking, 39–41
Computer security, 41–42
Computer software, 38–39
Criminal element, 2–3
Criminal law, 65–66
Criminal profiling, 65
Cross-site scripting attack (XSS attack), 10, 100
Cyber crime, cost of, 3–4
Cyber Mall, 99
Cyberattackers, 9
Cyberattacks, 2, 102–103
  methods, 7–9
CyberCorps, 123
Cybercrimes, 44, 65–66
Cybercriminals, 63–64, 66
  expert opinion, 96–97
  KSAs, 66
Cyberheroes, 63–64, 66
Cyberprofessionals, 66
Cybersecurity, 1–2, 63–64
  analysts, 99–100
  case-based scenario, 34–35, 61, 97–98
  certifications, 126–127
  challenges to global business and government, 15–19
  CMMC, 27–29
  competitions, 133–135
  cost of cyber crime, 3–4
  current and future cybersecurity roles and responsibilities, 69–70
  current cybersecurity job titles, 88
  current technologies, 37–42
  cyberattack methods, 7–9
  emerging technologies in, 42–59
  expert opinion, 32, 34, 59, 61
  frameworks of tomorrow, 27–29
  human resources and cybersecurity workforce of tomorrow, 70–88
  information systems, 37–38
  internships and co-ops, 135
  IT security governance, 24–27
  managing risk, 20–24

market for stolen data, 4–7
Matt Pascucci, Security Director, Evercore Group, 32–34
NICE Cybersecurity framework, 67–69
ranges, 133
recruiting cybersecurity professional, 84–85
retaining cybersecurity professional, 85–88
risk management, 21–22
sandboxes, 132
simulation, 139
software, 42
Solarium Report, 29
workers, 96
workforce, 9, 15, 69
Cybersecurity education at every level, 126–130
community colleges, 129
K-12 education, 127
professional certificates, 126–127
undergraduate and graduate degrees, 130
Cybersecurity Framework (CSF), 26–27
Cybersecurity jobs, 86–87
acquisition, 130–131
educational requirements, 131
Cybersecurity Maturity Model Certification (CMMC), 27, 29
Cybersecurity toolbox, 42, 99, 107, 112
border routers, 106
case-based scenario, 114–115
expert opinion, 112–114
firewalls, 106
intrusion detection, 102–103
IPSs, 104
network and packet analysis, 101
penetration testing, 103–104
perimeter security, 103
Secure Software Design, 106–107
UTM, 106
virus and malware protection, 101–102
Cybersecurity workforce, 7, 9, 13, 20–21, 117
case-based scenario, 145–146
developing, 124
educating, 118
gap, 18
NCWF, 118–124
of tomorrow, 37, 140, 145
CyberSeek, 14, 124, 126
Cyberspace, 65
Cyberspace Solarium Commission, 29

Dark web, 5–7
Data Science, 111–112, 141
Data trusts, 109

Deep Learning (DL), 43
Deep packet inspection (DPI), 101
Deep web, 5–6
Department of Defense (DoD), 27–28
Department of Defense Directive (DoDD), 118–119
  DoD Directive 8140.01, 120–122
Department of Homeland Security (DHS), 123–124
Desktop computers, 38
Devices, 38

E-readers, 38
Educational requirements, 131
Electrical and computer engineering, 142
Encryption, 99–100
Energy, 15–17
Entry-level cybersecurity jobs, 88, 90, 95
Equality in cybersecurity education, 139–140
Equifax, 4
Ethical hacking (see Penetration test(ing))
Event Manager, 100–101
Exactis, 4

Facebook, 4
Federal Information Security Modernization Act (FISMA), 22–23
FireMon, 100–101
Firewalls, 103, 106
  tools, 100–101
5G Core Network, 51
5G spectrum, 50–52
Flash drives, 38

General Data Protection Regulation (GDPR), 26
GitHub accounts, 96
Global business, challenges to, 15–19
Google, 49–50
Google's Android, 38–39
Governments, 18–19
  challenges to, 15–19
  drivers of cybersecurity education, 123
Graduate degrees, 130
Gramm–Leach–Bliley Act, 25

Hands-on preparation
  cybersecurity competitions, 133–135
  cybersecurity internships and co-ops, 135
  cybersecurity ranges, 133
  cybersecurity sandboxes, 132
  cybersecurity simulation, 139
  educational tools for, 132–139
Hardware security, 41–42
  solutions, 41–42

HaveIBeenPwned (HIBP), 97–98
Health Insurance Portability and Accountability Act (HIPAA), 25–26
Healthcare, 15–17
High-profile data breaches, 4
HITRUST Common Security Framework, 26–27
Host-based intrusion detection systems (HIDSs), 102–103
Human Capital Crisis in Cybersecurity, A, 15
Human resources and cybersecurity workforce of tomorrow, 70–88

IBM, 49–50
Industrial control systems (ICS), 54–55
Information systems, 37–38
  computer and network security, 41
  computer hardware, 38
  computer networking, 39–41
  computer software, 38–39
  cybersecurity toolbox, 42
  hardware and software security solutions, 41–42
  management, 26
Information technology (IT), 63–64
  examples of IT Security standards and frameworks, 26–27
  governance practices, 25–26
  security framework, 25
  security governance, 24–27
Input devices, 38
Institutional frameworks, 118
International Information Systems Security Certification Consortium (ISC2), 15
International Organization for Standardization, 26–27
Internet of Things (IoT), 13–14, 34, 39, 55–56, 109
Internet of Vehicles (IoV), 46, 56–57
Intrusion detection, 102–103
Intrusion detection systems (IDS), 44, 46, 103
Intrusion prevention systems (IPSs), 102–104
Invisible Internet Project (I2P), 5–6
ISO 27000 Series, 26–27
ISO 27002 Series, 25

ITU Global Cybersecurity Index, 18–19

Jeopardy format, 134–135
Josephson junctions, 49
Juniper Research, 3–4

K-12 education, 127
Kali Linux, 100, 104–105
Kaspersky Anti-Virus, 100
KeePass, 100
Keyboards, 38
Kismet, 100–101
Knowledge, skills, and abilities (KSAs), 66, 118
Knowledge Units (KUs), 123–125

Laptop computers, 38
Law, 143–144
Law Enforcement, 63–64
LinkedIn accounts, 96
Long Short Term Memory (LSTM), 45

Machine Learning (ML), 13–14, 42, 44, 112
  technologies, 32–33
Malicious cyberattacks, 2, 8–9
Man-in-the-middle attack (MITM attack), 10
Managed service provider (MSP), 104
Market for stolen data, 4–7
Marrakech markets, 5–6
McAfee Total Protection, 100
Metasploit, 100
Methods of operation (MO), 5, 8, 63–64
Mice, 38
Microsoft's Windows Mobile, 38–39
Mobile phones, 38

Nagios, 100
National Centers of Academic Excellence in Cyber Defense or Cyber Operations Education Programs (CAE-CD/CO), 118–119, 123–124
National Initiative for Cybersecurity Careers and Studies (NICCS), 126–127
National Initiative for Cybersecurity Education (NICE), 14, 66, 118
  Cybersecurity framework, 67–69
  Cybersecurity Roles, 71–81
  Workforce Framework for Cybersecurity, 69
National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NCWF), 118, 124

National Institute of Standards and Technology (NIST), 111, 123
National Institute of Standards and Technology's Risk Management Framework (NIST RMF), 22–23
National Science Foundation (NSF), 123
National Security Agency (NSA), 88, 123
Netsparker, 100
Network analysis, 101
Network analyzers, 100–101
Network intrusion detection, 99–100
Network intrusion detection systems (NIDS), 100–101
Network security
  computer and, 41
  monitoring, 99–100
    tools, 100
Nikto, 100
Noncybercrimes, 5
Nonfungible tokens (NFTs), 110–111
NordLocker, 100
Norton 360, 100
Norton AntiVirus, 100

Open web, 5–6
Operating systems, 38–39
Operation technology (OT), 54–55
Operations research, 142
Organizational losses, 1–2
OSSEC, 100
OWASP, 107

Packet analysis, 101
Packet analyzers, 100–101
Packet sniffers, 99–101
Paros Proxy, 100
Path traversal, 100
Payment Card Industry Data Security Standard (PCI DSS), 25
PCI DSS, 26
Pen test (see Penetration test(ing))
Penetration test(ing), 58, 99–100, 103–104
Perimeter security, 103
Pof, 100
Political science, 143
Ponemon Institute's Cost of a Data Breach Study, 3
Post quantum cryptography (PQC), 111
  algorithms, 50
Printers, 38
Professional certificates, 126–127
Protocol analyzers, 100–101
Public key infrastructure (PKI), 42

Quantum algorithms, 48–49
Quantum computing, 47–50
Quantum key distribution (QKD), 111
Quantum processor, 47–48
Quantum resistant encryption, 47–48
Quantum technologies, 111
Qubits, 47–48

Ransomware, 100
Recruitment process, 21, 83–84
RedSeal, 100–101
Retention, 83–84
Retention process, 21
Risk appetite, 20–21
Risk management, 20–24
Risk Management Framework (RMF), 22–23
Risk-based approach, 23

SAFECode, 107
Sandboxing, 132
Sarbanes–Oxley Act, 25–26
Scanners output devices, 38
Scholarship for Service (SFS), 123
Secure Software Design, 106–107
Secure Software Development Framework (SSDF), 107
Security Onion, 100–101
Security risk, 22
Security standards, regulations, and frameworks, 24–27
Singapore's national strategy, 18–19
Skilled cybersecurity workers, 13–14
Snort, 100–101
Social Security Numbers (SSNs), 34–35
Software development life cycle (SDLC), 107
Software security solutions, 41–42
Solarium Report, 7, 29
SolarWinds Security, 100–101
Speakers, 38
Specialized devices, 39–41
Splunk, 100
Spyware, 100
SQL injection, 100
SQLMap, 100
Storage devices, 38
Supercomputers, 48
Superposition, 49

Tablet computers, 38
Task, Knowledge, and Skill (TKS), 67
Tcpdump, 100–101
The Onion Router (Tor), 5–6, 100
Training data, 43–44
Transmission Control Protocol/Internet Protocol (TCP/IP), 7–8, 15, 17

Trojans, 100
TrueCrypt, 100
Tufin, 100–101

Under Armour, 4
Undergraduate degrees, 130
Unified Threat Management (UTM), 103, 106
United States Office of Personnel Management (OPM), 34–35

Vehicle security, 56–57
VeraCrypt, 100
Virtual private network (VPN), 106
Virus and malware protection, 101–102

Web vulnerability, 99–100
  scanning tools, 100
Wi-Fi, 39–41
Windump, 100–101
Wireshark, 100–101
Work roles, 67
Workforce Framework for Cybersecurity, 67
Worms, 100

Zeek, 100–101
Zero-trust networks, 52–54