

Index

■ A

Advanced persistent threats (APTs), 11
Architecture
 balanced controls, 72, 99–101
 definition, 99
 detective and preventative, 100
 detective controls, 99
 firewalls system, 99
 intrusion prevention systems, 99
 security business
 intelligence, 99–100
business needs, 90
BYOD, 88
cloud computing, 89
employee productivity, 91
hardware-enforced security, 91
IT consumerization, 88–89
privacy and regulatory
 requirements, 91
security zones, 92, 95–99
 critical data and resources, 95
 definition, 92
 devices and application
 types, 95, 96
 PEPs, 96
 selective zones, 97
 trusted zones, 97
 untrusted zones, 96–97
 user's device and location, 97, 98
threat landscape, 90–91
threat management, 88
traditional enterprise trust model, 91
trust calculation, 92–95
 access type, 92
 allow access, 92
 available controls, 92
 business partners, 95

 definition, 92
 destination score, 92
 devices and usage models, 92
 internal and external
 resources, 95
 policy decision point (PDP), 94
 source score, 92
user and data perimeters, 92, 101–102
 defenses and detective
 control, 101
 protect information, 101
 security, 101
 traditional network security, 101

■ B

Bring-your-own-device (BYOD), 88
Business benefits and risks
 baseline security, 109–110
 encryption, 109–110
 enhanced recovery, 110
 hardware acceleration, 110
 hardware-enforced, 109
 protected environments, 109
 security software, 109
building security, 108
context-aware experiences, 103
context-aware security, 110–112
 business intelligence and data
 protection, 112
 cloud security and context
 awareness, 111–112
 image recognition technology, 111
 portable devices, 111
 sensors and analytical
 tools, 110–111
contextual information, 109
mass-production strategy, 108

C, D

CISO

- attributes, 124
- chief information risk officer, 113–114
- foundational skills, 116
- junk food fear, 117–119
- leader, 122–123
- organizations outsource, 123
- sixth sense, 121–122
- storyteller, 116–117
- T-shaped individuals, 114
- Z-shaped individual, 115

Context-aware computing, 105

Context-aware technology, 81

Cybersecurity legislation, 6

Cybersecurity Watch Survey, 68

E

Emerging security capabilities

- accelerated encryption, 105
- adidas, 104
- business benefits and risks
 - (*see* Business benefits and risks)
- business intelligence and data, 107–108
- cloud computing, 107
- compute continuum, 107
- context-aware computing, 105
- context-aware security, 105
- context-aware technology, 104
- enterprise systems, 105
- hardware-enforced protection, 105
- LEGO brand, 104
- malicious purposes, 104
- Moore's law, 106
- shopper's smartphone, 106
- wireless NFC, 106

Enterprise information security, 105

External partnerships

- advantage of, 49
- benchmarking information, 54–55
- CISO, 53
- communities, 50
- community characteristics, 51–52
- community goals, 52
- corporate citizenship, 56
- enabling informal exchanges, 53
- FIRST, 54
- information-sharing relationships, 46

Intel's CISO, 50

legal implications, revealing security, 43

public-relations aspect, 43

regulations and standards, 55

security-related issues, 43

share security information, 44, 45

technology landscape, 44

threat landscape, 44

threats and vulnerabilities information, 52–53

tiered pyramid model, 46

F

"Find the Phish" game, 60, 61

Forum for Incident Response and Security Teams (FIRST), 54

G

Governance

dictatorial approach, 28

Intel's information risk, 31–32

IT governance archetypes, 30

IT policies, 29

MIT CISR, 28–29

H

Health Insurance Portability and Accountability Act (HIPAA), 7

I, J, K, L

Information security

balancing act, 5

blocking users' access, 5

business enable, 3

businesses and organization, 1

business risk, 14

company legal, 6–7

core competencies, 3

dynamic and flexible, 14

ecosystem, 6

implementing wireless networks, 3

incorporate privacy and regulatory compliance, 14

Intel's Group, 4, 5

Intel's internal team, 3

- malware, 1
- network boundary, 14
- personal smartphones, 4
- regulatory flood, 6–7
- safeguarding information, 5
- threat landscape, 1
- traditional mission
 - and vision, 1
- Information Sharing and Analysis Centers (ISACs), 53
- Installing wireless networks, 3
- Intel IT Emergency Response Process (ITERP), 42
- Intel’s information risk
 - governance, 31–32
- Intel’s legal and human
 - resources (HR) groups, 4
- Interdependent risks related, IT, 2
- Internal partnerships
 - business group managers, 41
 - corporate risk management, 40
 - corporate security, 41
 - far-reaching web, 33
 - fellow travelers, 33
 - finance group, 38–39
 - business groups, 38–39
 - internal audit, 39
 - SOX, 38
 - formal/informal, 33
 - human resources, 37–38
 - employee communications, 38
 - employee procedures, 37
 - internal investigations, 38
 - security policy, 37–38
 - information security group, 32, 33
 - ITERP, 42
 - legal, 34–36
 - business groups, 35–36
 - contracts, 34–35
 - data classification, 34
 - financial compliance, 35
 - intellectual property, 34
 - litigation, 34
 - privacy, 34
 - risk review boards, 32
 - standing committees, 32
- Internet-enabled car, 104
- Irrefutable Laws of Information Security, 12–14
- IT governance archetypes, 30

M

- Marketers, 3
- Massachusetts Institute of Technology Center for Information Systems Research (MIT CISR), 28–29
- Moore’s law, 106

N

- Near field communications (NFC), 106
- Network firewalls, 2
- Non-Intel managed systems (NIMS), 18

O

- Organization’s privacy commitment, 105

P, Q

- Perimeter
 - Bloomberg News, 59
 - building security, 60
 - business processes, 60
 - compliant behavior, 58
 - credit analyst, 59
 - customer financial data, 59
 - Cybersecurity Watch Survey, 68
 - disk encryption on laptops, 66
 - “Find the Phish” game, 60, 61
 - information security
 - professionals, 58
 - IT professional, 67–68
 - payoff, 63
 - physical and network, 57
 - privacy protection, 60
 - publishing security-related
 - articles, 62
 - security benefits, personal use, 65–66
 - self-motivated commitment, 58
 - smartphones access, 63
 - social media accounts, 60
 - technical controls, 69
 - unencrypted data, 67
- Playing War Games, 77–78
- Policy decision point (PDP), 94
- Policy enforcement points (PEPs), 96
- Product life cycle model
 - commodity—source code, 73
 - critical trends, 76

Product life cycle model (*cont.*)
disruptive trends, 76
emerging trends, 76
evolution of threats source, 73
highest-priority threats, 73
product manufacturing company, 74
security-related activity, 75
smartphone security threats, 74
sustained drivers, 76
threat analysis materials, 75

■ R

Radio Frequency Identification (RFID)
technology, 106

Rapid proliferation, information
and devices, 9–10

Regulatory environment, 2

Regulatory flood
cybersecurity legislation, 6
e-discovery, 9
financial regulations, 8
high-tech exports, 6
IT capabilities, 6
personalization versus privacy, 7–8
protecting personal information, 7
scope, 9
storage and protection, 6

Retail environment, 104

Right governance structure, 29–30

Risk misperception
communication, 23–25
asymmetry of information, 23
building credibility, 25
changing risk perceptions, 23
laptops, 24
pirating software, 23
decision makers, 20–21
economic and psychological factors, 15
employees, 16–18
inevitable bias, 21
organization's security posture, 16
risk assessment models, 22
security professionals, 15, 18–19
social-media site, 16

Roundabouts and stop signs, 64–65

■ S

Sarbanes-Oxley (SOX) Act, 8
Sarbanes-Oxley (SOX) compliance, 38
Security professionals, 104
Smartphones, 2
Spearphishing, 11

■ T, U, V, W, X, Y, Z

Threat landscape
APTs, 11
cybercrime online, 11
Irrefutable Laws of Information
Security, 12
stealthy malware, 11
Stuxnet creation, 11

Threats and vulnerabilities
Malware industry, 81–82
structured methods, 72–78
agents, 77
analyzing emerging threats, 72
blinkered security
perspective, 72
playing war games, 77–78
product life cycle model
(*see* Product life cycle model)
risk-sensing analysis, 73
risk-sensing strategy, 72
security team, 72
threat landscape, 72, 78–81
barriers, 79–80
broad-brush picture, 78
edge case insecurity, 80
obscurity, 80–81
phishing, 79
smartphones, 79
social engineering attacks, 79
web, attack surface, 82–84
embedded devices, 82
glimpse, 82
nontraditional devices, 82
security focus areas, 82
smartphones, 83–84
web applications, 84

Traffic metaphor, 64