

<i>Code</i>	<i>Description</i>
0	<i>Unclassified</i>
01	<i>Introduction</i>
02	<i>Taxonomy of INFOSEC Issues</i>
03	<i>Sources of Information</i>
04	<i>Copyright</i>
05	<i>Using IYIR</i>
06	<i>The INFOSEC UPDATE Course</i>
07	<i>Acknowledgements</i>
08	<i>About the Editor</i>
10	<i>HEADING: Computer Crimes (cases, indictments, convictions, sentences)</i>
11	<i>Breaches of confidentiality</i>
11.1	<i>Data leakage</i>
11.2	<i>Unauthorized disclosure</i>
11.3	<i>Data theft</i>
11.4	<i>Covert channels</i>
12	<i>Wiretapping, interception (not jamming; not govt/ law enforcement)</i>
12.1	<i>Wiretapping</i>
12.2	<i>Interception</i>
12.3	<i>Injection</i>
13	<i>Data diddling, data corruption, embezzlement</i>
13.1	<i>Data diddling</i>
13.2	<i>Data corruption & destruction</i>
13.3	<i>Embezzlement</i>
13.4	<i>Obsolescence</i>
14	<i>Viruses, virus-boaxes, Trojans (assembly level or macro: not ActiveX or Java)</i>
14.1	<i>Viruses</i>
14.2	<i>Worms</i>
14.3	<i>Virus/worms</i>
14.4	<i>Trojans & rootkits</i>
14.5	<i>Virus boaxes</i>
15	<i>Fraud (not embezzlement), extortion, slamming</i>
15.1	<i>Fraud</i>
15.2	<i>Extortion</i>
15.3	<i>Slamming</i>
16	<i>INFOWAR, industrial espionage, hacktivism</i>
16.1	<i>Industrial espionage</i>
16.2	<i>Industrial information systems sabotage</i>
16.3	<i>Infrastructure protection & homeland security</i>

<i>Code</i>	<i>Description</i>
16.4	<i>Military & government perspectives on INFOWAR</i>
16.5	<i>Hactivism</i>
16.6	<i>Disinformation, PSYOPS</i>
17	<i>Penetration, phreaking, crammng, uncapping (entering systems, stealing telephone or other services)</i>
17.1	<i>Penetration</i>
17.2	<i>Web vandalism</i>
17.3	<i>Phreaking, crammng, uncapping, theft of services</i>
18	<i>Theft/ loss of equipment (laptops, ATMs, computers, cables, network components)</i>
18.1	<i>Theft of equipment</i>
18.2	<i>Loss of equipment</i>
19	<i>Counterfeits, forgery (including commercial software/ music piracy)</i>
19.1	<i>Software piracy</i>
19.2	<i>Music piracy</i>
19.3	<i>Movies / TV piracy</i>
19.4	<i>Books / e-books piracy</i>
19.5	<i>Games piracy</i>
19.6	<i>Counterfeit currency, credit-cards, other negotiable tokens</i>
19.7	<i>Counterfeit legal or business documents</i>
19.8	<i>Plagiarism & cheating</i>
19.9	<i>Counterfeit products (hardware, clothing etc.)</i>
1A	<i>Criminal hacker scene (conventions, meetings, testimony, biographies, publications)</i>
1A1	<i>Criminal hacker conventions and meetings</i>
1A2	<i>Criminal hacker testimony in court or committees</i>
1A3	<i>Biographical notes on individual criminals (including arrests, trials)</i>
1A4	<i>Criminal hacker publications</i>
1A5	<i>Criminal hacker organizations</i>
1A6	<i>Criminal hacker psychology</i>
1B	<i>Pornography, Net-harm, cyberstalking, gambling, online auctions</i>
1B1	<i>Adult pornography</i>
1B2	<i>Child pornography</i>
1B3	<i>Pedophilia, kidnapping, Net-adoption fraud</i>
1B4	<i>Stalking & harassment</i>
1B5	<i>Gambling</i>
1B6	<i>Auctions</i>
1B7	<i>Hate groups, speech</i>
1B8	<i>Traffic in women, slavery</i>
1B9	<i>Non-virus hoaxes, urban myths</i>
1C	<i>Identity, impersonation, spoofing</i>

<i>Code</i>	<i>Description</i>
1C1	<i>Impersonation</i>
1C2	<i>Identity theft</i>
1C3	<i>Pseudonymity</i>
1C4	<i>Anonymity</i>
1C5	<i>Phishing</i>
1D	<i>Law Enforcement & Forensics (technology, organizations, proposals, litigation, rulings, judgements)</i>
1D1	<i>Organizations, cooperation for law enforcement</i>
1D2	<i>Technology for law enforcement</i>
1D3	<i>Litigation, legal rulings, judgements affecting law enforcement</i>
1D4	<i>Government funding for law enforcement</i>
20	<i>HEADING: Emerging Vulnerabilities & Defenses</i>
21	<i>Quality assurance failures including design flaws</i>
21.1	<i>General QA failures</i>
21.2	<i>Security product QA failures</i>
21.3	<i>Embedded processors</i>
21.4	<i>SCADA (supervisory control and data acquisition) systems, vehicle controls</i>
21.5	<i>Robots, botnets</i>
22	<i>Availability problems</i>
22.1	<i>DoS attacks</i>
22.2	<i>DDoS attacks</i>
22.3	<i>DoS countermeasures</i>
22.4	<i>Accidental availability disruptions</i>
23	<i>Internet tools</i>
23.1	<i>Java</i>
23.2	<i>Javascript</i>
23.3	<i>ActiveX</i>
23.4	<i>HTML, XML, browsers</i>
23.5	<i>E-mail & instant messaging or chat</i>
23.6	<i>Web-site infrastructure, general Web security issues</i>
23.7	<i>VoIP</i>
23.8	<i>SMS</i>
23.9	<i>PERL, CGI scripts</i>
24	<i>Operating systems, network operating systems, TCP/IP problems (alerts & improvements)</i>
24.1	<i>Windows 9x/Me</i>
24.2	<i>Windows NT/2K/XP</i>
24.3	<i>UNIX flavors</i>
24.4	<i>TCP/IP & HTTP</i>
24.5	<i>LAN OS</i>

<i>Code</i>	<i>Description</i>
24.6	<i>WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax</i>
24.7	<i>SWDR (Software-defined radio)</i>
24.8	<i>MAC OS</i>
24.9	<i>Peer-to-peer networking</i>
24.A	<i>Secure processors</i>
24.B	<i>Robust systems (hw / sw)</i>
25	<i>Computer remote control & disruption</i>
25.1	<i>Remote control, RATs, reprogramming, auto-updates</i>
25.2	<i>Jamming</i>
25.3	<i>RFI, HERF, EMP/T</i>
26	<i>Health effects of electronic equipment (phones, screens, etc.)</i>
26.1	<i>Radiation</i>
26.2	<i>Toxic materials</i>
26.3	<i>Heat</i>
26.4	<i>Distraction</i>
27	<i>Security tools</i>
27.1	<i>Vulnerability assessment</i>
27.2	<i>Port scans</i>
27.3	<i>Intrusion detection systems</i>
27.4	<i>Firewalls & other perimeter defenses</i>
27.5	<i>Honeypots</i>
27.6	<i>Honeynets</i>
27.7	<i>Anti-malware technology</i>
28	<i>Automated surveillance</i>
28.1	<i>Spyware, Web bugs & cookies</i>
28.2	<i>Scumware</i>
28.3	<i>Keystroke loggers</i>
28.4	<i>Cell/mobile phones/GPS/cameras</i>
28.5	<i>Serial numbers</i>
28.6	<i>RFID tags</i>
29	<i>Sociology of cyberspace</i>
29.1	<i>Addiction, games & violence</i>
29.2	<i>Cyberdating & cybersex</i>
29.3	<i>Digital divide</i>
29.4	<i>Online & electronic voting</i>
29.5	<i>Online legal proceedings</i>
29.6	<i>Flash crowds, social e-links</i>
29.7	<i>Outsourcing</i>

<i>Code</i>	<i>Description</i>
30	<i>HEADING: Management & Policy</i>
31	<i>The state of information security & technology</i>
31.1	<i>Surveys, studies, audits of security</i>
31.2	<i>Estimates, guesses, predictions, forecasts concerning security</i>
31.3	<i>New technology with security implications</i>
31.4	<i>Outsourcing</i>
32	<i>Censorship, indecency laws, 1st amendment (law)</i>
32.1	<i>Censorship in the USA</i>
32.2	<i>Censorship outside the USA</i>
33	<i>Policies, risk analysis, risk management</i>
33.1	<i>Acceptable use policies</i>
33.2	<i>Spam, spim, spit & splogs</i>
33.3	<i>Authorization, access controls</i>
33.4	<i>Risk analysis & management</i>
34	<i>Net filters, monitoring (technologies)</i>
34.1	<i>Net filters</i>
34.2	<i>Usage monitoring, audit trails (employees, children)</i>
35	<i>DNS conflicts, trademark violations (Net, Web)</i>
35.1	<i>Cybersquatting</i>
35.2	<i>Trademarks vs DNS</i>
35.3	<i>Politics & management of the DNS</i>
36	<i>Responses to intrusion</i>
37	<i>Education in security & ethics</i>
37.1	<i>Elementary & middle school programs</i>
37.2	<i>High school programs</i>
37.3	<i>Undergraduate programs</i>
37.4	<i>Master's programs</i>
37.5	<i>Doctoral programs</i>
37.6	<i>Industry courses</i>
37.7	<i>Conferences</i>
37.8	<i>Web sites</i>
37.9	<i>White papers</i>
37.A	<i>Books</i>
38	<i>Consumer/employee / individual privacy, profiling & surveillance (non-governmental)</i>
38.1	<i>Consumer / employee / individual profiling & surveillance (non-governmental)</i>
38.2	<i>Trade in personal information</i>
38.3	<i>Industry efforts for individual privacy protection</i>
38.4	<i>International agreements on security, individual privacy, Net law</i>

<i>Code</i>	<i>Description</i>
38.5	<i>EU case law, legislation & regulation concerning individual privacy (not govt surveillance)</i>
38.6	<i>US case law, legislation & regulation concerning individual privacy (not govt surveillance)</i>
38.7	<i>Other case law, legislation & regulation concerning individual privacy (not govt surveillance)</i>
38.8	<i>Law enforcement & privacy rights</i>
38.9	<i>Medical information & HIPAA</i>
40	<i>HEADING: Defensive Technology, Law of E-commerce, Intellectual Property</i>
41	<i>Cryptanalysis techniques & tools</i>
42	<i>Crypto algorithms (weakness, brute-force attacks, implementation flaws)</i>
42.1	<i>Crypto algorithm weaknesses</i>
42.2	<i>Brute-force attacks</i>
42.3	<i>Crypto product implementation flaws</i>
43	<i>I&A products (tokens, biometrics, passwords, Kerberos)</i>
43.1	<i>Tokens</i>
43.2	<i>Biometrics</i>
43.3	<i>Passwords</i>
43.4	<i>Kerberos</i>
43.5	<i>Single sign-on</i>
43.6	<i>E-mail authentication (e.g., SPF & SenderID)</i>
44	<i>Encryption algorithms, products (including steganography)</i>
44.1	<i>Crypto algorithms</i>
44.2	<i>Crypto products</i>
44.3	<i>Steganography</i>
45	<i>E-commerce security, digital signature, products, digital cash, e-payments</i>
45.1	<i>PKI (Digital signatures / certificates)</i>
45.2	<i>Digital cash</i>
45.3	<i>Micropayments</i>
45.4	<i>E-payments; e.g., credit-cards, e-brokers</i>
45.5	<i>Digital-rights management (DRM); e.g., copy protection, digital watermarks</i>
45.6	<i>Smart cards and other e-commerce security measures</i>
45.7	<i>Sales taxes on Internet commerce</i>
45.8	<i>E-commerce laws</i>
45.9	<i>E-shopping carts</i>
46	<i>Cryptography exports from US; Key escrow</i>
47	<i>US computer-crime laws</i>
48	<i>Foreign cyberlaws (not cases or sentences)</i>
48.1	<i>Non-US cryptography laws</i>
48.2	<i>Non-US computer-crime laws</i>
48.3	<i>Non-US intellectual property laws</i>

<i>Code</i>	<i>Description</i>
49	<i>Government surveillance, legislation regulating govt surveillance, case-law</i>
49.1	<i>US government surveillance of citizens</i>
49.2	<i>Non-US government surveillance of citizens</i>
4A	<i>Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality</i>
4A1	<i>Framing</i>
4A2	<i>Pointing, linking, deep linking, metatext</i>
4A3	<i>Jurisdiction</i>
4A4	<i>Blocking</i>
4A5	<i>Archives</i>
4A6	<i>Libel</i>
4A7	<i>Spam</i>
4A8	<i>Liability</i>
4A9	<i>Net neutrality</i>
4B	<i>Intellectual property: patents, copyrights (law)</i>
4B1	<i>Copyrights</i>
4B2	<i>Patents</i>
4B3	<i>Reverse engineering</i>
4B4	<i>EULA (End-user license agreements)</i>
4B5	<i>Trademarks</i>
4C	<i>Security paradigms, risk management, site-security certification, professional certification</i>
4C1	<i>Paradigms, security standards</i>
4C2	<i>Risk management methodology & tools</i>
4C3	<i>Certification of site security, privacy protection</i>
4C4	<i>Professional certification in security, auditing</i>
4C5	<i>Academic/Industry/Vendor/Govt efforts</i>
4D	<i>Funny / miscellaneous</i>
T	TEMPORARY PLACEHOLDER