References

1. Accenture: 2017 Cost of Cyber Crime Study. Tech. rep. (2017). Web publication: https://www.accenture.com/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf [Accessed 22-June-2023]
2. Alberts, C., Dorofee, A.: OCTAVE Method Implementation Guide Version 2.0, Volume 1: Introduction. Tech. rep., Software Engineering Institute, Carnegie Mellon University (2001). Web publication: https://resources.sei.cmu.edu/asset_files/UsersGuide/2001_012_001_51564.pdf [Accessed 22-June-2023]
3. Alberts, C., Dorofee, A., Stevens, J., Woody, C.: Introduction to the OCTAVE approach. Tech. rep., Software Engineering Institute, Carnegie Mellon University (2003). Web publication: https://resources.sei.cmu.edu/asset_files/UsersGuide/2003_012_001_51556.pdf [Accessed 22-June-2023]
4. Ale, B.: Risk: An Introduction. Routledge (2009). ISBN 978-0-415-49090-0
5. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M.J., Levi, M., Moore, T., Savage, S.: Measuring the cost of cybercrime. In: B. Schneider (ed.) Economics and Information Security and Privacy III, pp. 265–300. Springer Verlag (2012). ISBN 978-146141980
6. Arief, U., Bin Adzmi, M.A.: Understanding cybercrime from its stakeholders' perspectives: Part 2 – defenders and victims. IEEE Security and Privacy **13**(2), 84–88 (2015). DOI 10.1109/MSP.2015.44
7. Arief, U., Bin Adzmi, M.A., Gross, T.: Understanding cybercrime from its stakeholders' perspectives: Part 1 – attackers. IEEE Security and Privacy **13**(1), 71–76 (2015). DOI 10.1109/MSP.2015.19
8. Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Version wp248 rev.01. European Commission DG Justice (2017). Web publication: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711 [Accessed 22-June-2023]
9. Ayers, R., Brothers, S., Jansen, W.: Guidelines on mobile device forensics. NIST Special Publication SP800-101 Rev.1, National Institute of Standards and Technology (2014)
10. Barth, A.: RFC 6265: HTTP State Management Mechanism (2011)
11. Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., Scarfone, K.: Guide for cybersecurity event recovery. NIST Special Publication SP800-184, National Institute of Standards and Technology (2016)
12. Booz Allan Hamilton: Software security assessment tools review. Tech. rep., US NAVSEA (2009). Web publication: https://samate.nist.gov/docs/NAVSEA-Tools-Paper-2009-03-02.pdf [Accessed 22-June-2023]
13. Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R.: Introducing OCTAVE Allegro: Improving the information security risk assessment process. Tech. Rep. CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon University (2007). Web pub-

R. Sharp, *Introduction to Cybersecurity*, Undergraduate Topics in Computer Science,
https://doi.org/10.1007/978-3-031-41463-3

lication: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf [Accessed 22-June-2023]

14. Casey, E., Stellatos, G.J.: The impact of full disk encryption on digital forensics. ACM SIGOPS Operating Systems Review **42**(3), 93–98 (2008)
15. Comer, D.E.: The Internet Book: Everything you need to know about computer networking and how the Internet works, fourth edn. Pearson (2007). ISBN 978-0-13-233553-9
16. Comer, D.E.: Computer Networks and Internets, sixth edn. Pearson (2014). ISBN 978-0-13-358793-7
17. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, revision 4. Publication CCMB-2012-09-001 (2012). Web publication: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf [Accessed 22-June-2023]
18. COSO: Internal Control – Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission (2013). ISBN 978-1-93735-239-4
19. Council of Europe: European Treaty Series no. 185: Convention on Cybercrime (2001)
20. Council of Europe: Council of Europe Treaty Series no. 196: Council of Europe Convention on the Prevention of Terrorism (2005)
21. Creative Commons: Attribution 2.5 Generic. Web publication: https://creativecommons.org/licenses/by/2.5/legalcode [Accessed 22-June-2023]
22. Creative Commons: Attribution 3.0 Unported. Web publication: https://creativecommons.org/licenses/by/3.0/legalcode [Accessed 22-June-2023]
23. Crocker, D., Hansen, T., S.Kucherawy, M.: RFC 6376: Domain Keys Identified Mail (DKIM) Signatures (2013). Internet Standard STD 76.
24. Dahse, J., Holz, T.: Simulation of built-in PHP features for precise static code analysis. In: NDSS'14: Proceedings of the 2014 Network and Distributed System Security Symposium. Internet Society (2014)
25. Dhamija, R., Tygar, J., Hearst, M.: Why phishing works. In: R. Grinter, et al. (eds.) CHI2006: Proceedings of SIGCHI Conference on Human Factors in Computing Systems, Montréal, Canada, pp. 581–590. ACM (2006)
26. Dunkelman, O., Keller, N., Shamir, A.: A practical-time attack on the KASUMI cryptosystem used in GSM and 3G telephony. In: Advances in Cryptology – CRYPTO 2010, *Lecture Notes in Computer Science*, vol. 6223, pp. 393–410. Springer-Verlag (2010)
27. Dworkin, M.: Recommendation for block cipher modes of operation. NIST Special Publication SP800-38A, National Institute of Standards and Technology (2001)
28. European Commission: Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries. Web publication: https://commission.europa.eu/system/files/2021-06/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf (2021). [Accessed 22-June-2023]
29. European Data Protection Board: Guidelines 3/2019 on processing of personal data through video devices, version 2.0. Tech. rep., European Commission, Brussels (2020). Web publication: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf [Accessed 22-June-2023]
30. European Union: Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (1999)
31. European Union: Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. (2014)
32. European Union: Regulation 2016/679 of the European Parliament and of the Council: General Data Protection Regulation (2016)
33. Evans, D., Larochelle, D.: Improving security using extensible lightweight static analysis. IEEE Software pp. 42–51 (2002)
34. Falliere, N., O Murchu, L., Chien, E.: W32.Stuxnet Dossier. Symantec Corporation, 1.4 edn. (2011). Web publication: https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en [Accessed 22-June-2023]

35. Felt, A.P., Chin, E., Hanna, S., Song, D., Wagner, D.: Android permissions demystified. In: CCS'11, pp. 627–637. ACM (2011)
36. Ferguson, N., Schneier, B., Kohno, T.: Cryptography Engineering: Design Principles and Practical Applications. Wiley (2010). ISBN 978-0-470-47424-2
37. FireEye, Inc.: Redline User Guide, 2.0 edn. (2020). Web publication: `https://fireeye.market/assets/apps/211364/documents/877936_en.pdf` [Accessed 22-June-2023]
38. Frankel, S., Hoffman, P., Orebaugh, A., Park, R.: Guide to SSL VPNs. NIST Special Publication SP800-113, National Institute of Standards and Technology (2008)
39. Freed, N., Borenstein, N.S.: RFC 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies (1996)
40. Freed, N., Borenstein, N.S.: RFC 2046: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types (1996)
41. Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest We Remember: Cold Boot Attacks on Encryption Keys. In: Proceedings of the 17th USENIX Security Symposium, pp. 45–60. Usenix (2008)
42. Housley, R.: RFC 5652: Cryptographic Message syntax (CMS) (2009). Internet Standard STD70.
43. Hovemeyer, D., Pugh, W.: Finding more null pointer bugs, but not too many. In: PASTE'07: Proceedings of the 7th ACM SIGPLAN-SIGSOFT Workshop on Program Analysis for Software Tools and Engineering, San Diego, pp. 9–14. ACM (2007)
44. IANA: Uniform Resource Identifier (URI) Schemes (2022). Web publication: `https://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml` [Accessed 22-June-2023]
45. International Standards Organisation: International Standard ISO11172-2: Information Technology – Coding of Moving Pictures and Associated Audio for Digital Storage Media at up to about 1,5 Mbit/s – Part 2: Video (1993)
46. International Standards Organisation: International Standard ISO10918-1: Information Technology – Digital compression and coding of continuous-tone still images – Part 1: Requirements and guidelines (1994)
47. ISACA (ed.): COBIT5 for Information Security. Information Systems Audit and Control Association (2012). ISBN 978-1-60420-255-7
48. ISO: ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management. International Organization for Standardization, second edn. (2011)
49. ISO: ISO/IEC 27002:2013 Information Technology – Security Techniques – Code of Practice for Information Security Management. International Organization for Standardization (2013)
50. ITU-T: Recommendation G.711: Pulse Code Modulation (PCM) of Voice Frequencies (1972)
51. ITU-T: Recommendation X.520: The Directory: Selected Attribute Types (1993)
52. ITU-T: Report on the e-commerce survey conducted in the framework of World Telecommunication Day 1999 (1999). Web publication: `https://www.itu.int/newsarchive/wtd/1999/report.html` [Accessed 22-June-2023]
53. Jones, J.A.: An Introduction to Factor Analysis of Information Risk. Tech. rep., Risk Management Insight LLC (2006). Web publication: `https://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf` [Accessed 22-June-2023]
54. Jonsson, J., Kaliski, B.: RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 (2003)
55. Kahneman, D.: Thinking, Fast and Slow. Penguin Books, London (2012). ISBN 978-0-141-03357-0
56. Kahneman, D., Slovic, P., Tversky, A. (eds.): Judgment under Uncertainty: Heuristics and Biases. Cambridge University Press, Cambridge (1982). ISBN 0-521-28414-7
57. Kent, K., Chevalier, S., Grance, T., Dang, H.: Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication SP800-86, National Institute of Standards and Technology (2006)
58. Kitterman, S.: RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1 (2014)

59. Kosinski, M., Stillwell, D., Graepel, T.: Private traits and attributes are predictable from digital records of human behaviour. Proceedings of the National Academy of Sciences **110**(15), 5802–5805 (2013)
60. Kurose, J.F., Ross, K.W.: Computer Networking – A Top-Down Approach Featuring the Internet, seventh edn. Addison-Wesley (2016). ISBN 978-0-13-359414-0
61. Lewand, R.: Cryptological Methematics. Mathematical Association of America (2000). ISBN 98-0-883-85719-7
62. Ligh, M.H., Case, A., Levy, J., Walters, A.: The Art of Memory Forensics. John Wiley (2014)
63. Mandiant: APT1. Mandiant Intelligence Center (2013). Available from archive at: `https://web.archive.org/web/20211008023335/https://www.mandiant.com/media/9941/download` [Accessed 22-June-2023]
64. McAfee: Net losses: Estimating the global cost of cybercrime. Tech. rep., Center for Strategic and International Studies (2014)
65. Mitnick, K.D., Simon, W.L.: The Art of Deception: Controlling the Human Element of Computer Security. Wiley Books (2003). ISBN 978-0-7645-4280-0
66. Moriarty, K.M., Nystrom, M., Parkinson, S., Rusch, A., Scott, M.: RFC 7292: PKCS #12: Personal Information Exchange Syntax v1.1 (2014)
67. Morris, R., Thompson, K.: Password security: A case history. Communications of the ACM **22**(11), 594–597 (1979)
68. NIST: Framework for improving critical infrastructure cybersecurity, version 1.1. Tech. rep., National Institute of Standards and Technology (2018). Web publication: `https://csrc.nist.gov/publications/detail/white-paper/2018/04/16/cybersecurity-framework-v11/final` [Accessed 22-June-2023]
69. Nystrom, M., Kaliski, B.: RFC 2986: PKCS #10: Certification Request Syntax Specification Version 1.7 (2000)
70. OWASP Foundation: OWASP Top 10 – 2021. Tech. rep., Open Web Application Security Project (2021). Web publication: `https://owasp.org/Top10/` [Accessed 22-June-2023]
71. Patterson, D.A., Hennessy, J.L.: Computer Organization and Design – The Hardware/Software Interface, sixth edn. Morgan Kaufmann (2020). ISBN 978-0-12-820109-1
72. Ramsdell, B., Turner, S.: RFC 5751: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification (2010)
73. Reschke, J.F.: RFC 7617: The 'Basic' HTTP Authentication Scheme (2015)
74. Robshaw, M., Billet, O. (eds.): New Stream Cipher Designs – The eSTREAM Finalists, *Security and Cryptology*, vol. 4986. Springer-Verlag (2008). ISBN 978-3-540-68351-3
75. Rogers, R.W.: Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In: J. Cacioppo, R. Petty (eds.) Social Psychophysiology, pp. 153–176. Guilford Press, New York (1983)
76. Royal Society: Risk: Analysis, perception and management. Report of a Royal Society Working Group, Royal Society, London (1992)
77. Schmitt, N. (ed.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press (2017). ISBN 978-1-316-63037-2
78. Schneier, B.: Applied Cryptography, second edn. Wiley (1996). ISBN 978-0-471-11709-4
79. Sciberras, A.: RFC 4519: Lightweight Directory Access Protocol (LDAP): Schema for User Applications (2006)
80. Seltzer, W., Anderson, M.: Ethical issues in using statistics, statistical methods, and statistical sources in work related to homeland security. In: Encyclopedia of Quantitative Risk Analysis and Assessment, vol. 2. John Wiley (2008). ISBN: 978-0-470-03549-8
81. Shekh-Yusef, R., Ahrens, D., Bremer, S.: RFC 7616: HTTP Digest Access Authentication (2015)
82. Singh, S.: The Code Book: The Secret History of Codes and Code-breaking. Fourth Estate (1999). ISBN 978-1-857-02889-8
83. Smart, N.: Cryptography Made Simple. Springer-Verlag (2016). ISBN 978-3-319-21935-6
84. Stallings, W., Brown, L.: Computer Security: Principles and Practice, fourth edn. Pearson (2018). ISBN 978-0-134-79410-5

85. Stinson, D.R., Paterson, M.: Cryptography: Theory and Practice, fourth edn. Chapman & Hall/CRC (2018). ISBN 978-1-138-19701-5
86. Tanenbaum, A.S., Austin, T.: Structured Computer Organization, sixth edn. Pearson (2012). ISBN 978-0-13-291652-3
87. Tews, E., Weinmann, R.P., Pyshkin, A.: Breaking 104 bit WEP in less than 60 seconds. In: Proceedings of the 8th International Workshop on Information Security Applications (WISA 2007), *Lecture Notes in Computer Science*, vol. 4867, pp. 188–202. Springer-Verlag (2007)
88. The Tor Project: Tor: Overview. Web publication: `https://www.torproject.org/about/overview.html.en` (undated). [Accessed 22-June-2023]
89. Todorov, A., Baron, S.G., Oosterhof, N.N.: Evaluating face trustworthiness; A model based approach. Social Cognitive and Affective Neuroscience **3**(2), 119–127 (2008)
90. del Torto, D., Elkins, M., Levien, R., Roessler, T.: RFC 3156: MIME Security with OpenPGP (2001)
91. US National Security Agency: NSA ANT catalog. Web publication (2013). Original publication date unknown. Available from Wikimedia Commons: `https://commons.wikimedia.org/wiki/Category:NSA_ANT` [Accessed 22-June-2023]
92. Verizon: 2016 Data Breaches Investigations Report. Tech. rep. (2016). Web publication: `https://www.verizon.com/business/resources/reports/DBIR_2016_Report.pdf` [Accessed 22-June-2023]
93. Verizon: 2021 Data Breaches Investigations Report. Tech. rep. (2021). Web publication: `https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf`
94. Weirich, D., Sasse, M.A.: Pretty Good Persuasion: A first step towards effective password security for the Real World. In: NSPW'01: Proceedings New Security Paradigms Workshop 2001, Cloudcroft, New Mexico, pp. 137–143. ACM Press (2001)
95. WHATWG: HTML – Living Standard. Web publication: `https://html.spec.whatwg.org/print.pdf` (2022). [Accessed 22-JUne-2023. Always the latest updated version.]
96. Wheeler, D.A.: Flawfinder (2001). Web publication: `https://www.dwheeler.com/flawfinder` [Accessed 22-June-2023]
97. Wheeler, D.A.: Secure Programming HOWTO, v3.72 edn. (2015). Web publication: `https://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO.pdf` [Accessed 22-June-2023]
98. Wheeler, D.A.: How to Prevent the next Heartbleed (2020). Revised edition, originally issued 2014. Web publication: `https://dwheeler.com/essays/heartbleed.html` [Accessed 22-June-2023]
99. Wikipedia contributors: List of operating systems — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=List_of_operating_systems&oldid=1160973695` (2023). [Online; accessed 21-June-2023]
100. Williams, J.: ACPO Good Practice Guide for Digital Evidence. Tech. rep., Association of Chief Police Officers (2012). Web publication: `https://athenaforensics.co.uk/wp-content/uploads/2019/01/National-Police-Chiefs-Council-ACPO-Good-Practice-Guide-for-Digital-Evidence-March-2012.pdf` [Accessed 22-June-2023]
101. Williamson, A.M., Feyer, A.M., Cairns, D., Biancotti, D.: The development of a measure of safety climate: The role of safety perceptions and attitudes. Safety Science **25**(1), 15–27 (1997)