B N H
. A I

References

Burt, A. and Hall, P. *What to Do When AI Fails*. O'Reilly Media, available at https://www.oreilly.com/radar/what-to-do-when-ai-fails/.

Cichonski, P. et al. *Computer Security Incident Handling Guide*. NIST, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Crowley, C. et al. *APT Incident Handling Checklist*. SANS, available at https://www.sans.org/media/score/checklists/APT-IncidentHandling-Checklist.doc.

Gill, N., Hall, P., Montgomery, K., and Schmidt, N. *A Responsible Machine Learning Workflow with Focus on Interpretable Models, Post-hoc Explanation, and Discrimination Testing*. Information 11(3), available at https://www.mdpi.com/2078-2489/11/3/137.

Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. Federal Financial Institutions Examination Councils, available at https://www.fdic.gov/news/news/financial/2005/fil2705.pdf.

Hall, P. *Proposals for Model Vulnerability and Security*. O'Reilly Media, available at https://www.oreilly.com/content/proposals-for-model-vulnerability-and-security/.

Kosseff, Jeff. *The Cybersecurity Privilege*. I/S: A Journal of Law and Policy for the Information Society, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3225782.

McGraw, G., Figueroa, F., Shepardson, V., and Bonett, R. *An Architectural Risk Analysis of Machine Learning Systems: Toward More Secure Machine Learning*. Berryville Institute for Machine Learning, available at https://berryvilleiml.com/results/.

Stalla-Bourdilon, S., Leong, B., Hall, P., and Burt, A. *Warning Signs: The Future of Privacy and Security in an Age of Machine Learning*. Future of Privacy Forum, available at https://fpf.org/wp-content/uploads/2019/09/FPF_WarningSigns_Report.pdf.

Supervisory Guidance on Model Risk Management, Board of Governors of the Federal Reserve System & Office of the Comptroller of the Currency, available at https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf.