May 8, 2018

Presidential Executive Order (EO) 13800
Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
Supporting Transparency in the Marketplace
Summary

Overview

Presidential Executive Order (EO) 13800 - *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, required the Secretary of the Department of Homeland Security (DHS), in coordination with the Secretary of Commerce to provide a report to the President by August 9, 2017 that examines the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices, with a focus on publicly traded critical infrastructure entities.

The report was developed through a collaborative interagency process. Due to the 90-day timeframe prescribed, the report focused on the identification of existing Federal policies and practices; identification and review of third-party evaluations of transparency practices and systems from independent sources; and limited private industry engagement available in the short-timeframe. DHS conducted a literature review of secondary sources addressing the sufficiency of existing Federal policies and practices in promoting transparency of cybersecurity risks and risk management practices, and the effectiveness of transparency systems, in general, in advancing policy goals. There were 96 different sources identified as part of the literature review, and several Federal policies and practices identified. While no formal tasking resulted from the development of this report, the associated findings provide insight into the effectiveness of transparency systems; the sufficiency of existing Federal policies and practices; and informs future policy discussions regarding market transparency and improving cybersecurity outcomes.

Effectiveness of Transparency Systems

Transparency systems in general. Beginning with transparency systems in general, the literature reviewed finds that of the various forms of transparency systems, *those that embed information into the decision processes of both information users and disclosers are highly effective*. These transparency systems, such as corporate financial disclosure, restaurant hygiene quality cards, and mortgage lending reporting, are highly effective in that they lead to consumers obtaining relevant, disclosed information and then enables making choices that lead disclosers to alter their behavior and make behavior more congruent with policy intentions. For example, corporate financial disclosure leads to institutional and individual investors using key indicators from quarterly and annual reports to inform stock purchases and sales. Company managers, in turn, track investor responses to their financial disclosures as a routine practice and respond to perceived investor concerns.

Cybersecurity transparency systems. Moving more specifically to cybersecurity transparency systems, the identified Federal policies and practices spanned all critical infrastructure sectors, with sector-specific policies in the Communications; Energy; Financial Services; Healthcare and Public Health; and Nuclear Reactors, Materials, and Waste sectors. The review of current and existing policies reveal that although some progress has been made in recent years, limitations remain and there is much to be done to improve transparency in cybersecurity risk management. The questions raised below will inform future policy considerations.

Suggestions for Further Research and Policy Considerations

The examination of the sufficiency of existing federal policies and practices identified a number of questions that warrant further research and policy considerations, including:

1. Can publicly-traded companies disclose meaningful information to investors without providing information that would be useful to adversaries?

2. Can federal policies and practices guide critical infrastructure entities in finding a balance between disclosing meaningful information that promotes transparency of cybersecurity risks and risk management practices without disclosing information that could be useful to adversaries?

3. What is the correlation between disclosure (or lack thereof) and cybersecurity breaches in publicly traded companies?
4. How can existing potential disclosure policies help foster efficient investment in security without the need for further regulation?
5. How can government initiatives and public-private partnerships support effective understanding and communication of risk-reducing investments?
6. Independent of federal policies and practices, to what extent do incentives exist to encourage critical infrastructure entities to be transparent about cybersecurity risks and risk management practices? To what degree do such incentives have the potential for promoting cybersecurity risk management among these entities?
7. To what degree do critical infrastructure entities have effective means for providing input to the federal government on its policies and practices, through membership on steering committees, in councils, as part of public-private partnerships, and through other channels? How might this type of engagement by critical infrastructure entities encourage these entities to become more transparent about cybersecurity risk and risk management practices?
8. Do market practices other than required public disclosure – such as due diligence, insurance underwriting, or corporate auditing – support appropriate transparency in the marketplace regarding cybersecurity risk and risk management practices?
9. How does reporting cyber incidents to, and cooperating with, law enforcement promote market transparency, and how can federal policies and practices encourage reporting of cybersecurity incidents to appropriate law enforcement authorities?

Reference List

Acquisti, A., Friedman, A., & Telang, R. (2006). Is There A Cost To Privacy Breaches? An Event Study. Proceedings of Twenty Seventh International Conference on Information Systems. Retrieved from http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf

Allianz. (2016). Allianz Risk Barometer: Top Business Risks 2016. Retrieved from http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf

American Bankers' Association. Data Security & Customer Notification Requirements for Banks. Retrieved from http://www.aba.com.

Avellan, N. (2014). The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America. Washburn Law Journal, 54(1): 193-226.

Bailey, T., Brandley, J., & Kaplan, J. (December 2013). How good is your cyberincident-response plan? McKinsey & Company. Retrieved from http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/how-good-is-your-cyberincident-response-plan

Bakker, T. G., & Streff, K. (Jul 2016). Accuracy of Self Disclosed Cybersecurity Risks of Large U.S. Banks. Journal of Applied Business and Economics, 18 (3): 39-51.

Ball, R. (2001). Infrastructure requirements for an economically efficient system of public financial reporting and disclosure. Brookings-Wharton Papers on Financial Services. Washington, DC: Brookings Institution.

Bambauer, D. (2011). Rules, Standards, and Geeks. Brooklyn Journal of Corporate Finance & Commercial Law, Brooklyn Law School, Legal Studies Paper No. 223: 49-64. Retrieved from https://ssrn.com/abstract=1792824

Benston, G.J. (1973). Required disclosure and the stock market: An evaluation of the Securities Exchange Act of 1934. The American Economic Review, 63(1), 132–155.http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=4504810&site=ehost-live

Bonner, L. (2012). Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches. Washington University Journal of Law Policy, 40: 257-278.

Botosan, C.A. (1997). Disclosure level and the cost of equity capital. The Accounting Review, 72, 323–349. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=9709240185&site=ehost-live

Bruening, P., & Culnan, M. (2016). Through Glass Darkly: From Privacy Notices to Effective Transparency. North Carolina Journal of Law Technology, 17(4): 515-580.

Buckman, J., Bockstedt, J. C., Hashim, M. J., & Woutersen, T. (2017). Do Organizations Learn from a Data Breach? Presented at WEIS 2017, La Jolla, CA, 2017. Retrieved from http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_55.pdf

Burbank, C. (2017). Significant Changes to HIPAA Effective March 26, 2013. Miller & Martin PLLC. Retrieved from http://www.jdsupra.com/legalnews/significant-changes-to-hipaa-effective-m-51197/

Burdon, M., Low, R., & Reid, J. (2010). Encryption safe harbours and data breach notification laws. Computer Law & Security Review, 26(5): 520-534.

Bushman, R.M., & Smith, A.J. (2001). Financial accounting information and corporate governance. Journal of Accounting and Economics, 32, 237–333.

Camp, L. J., and Johnson, M. E. (2012). The Economics of Financial and Medical Identity Theft. Springer Science & Business Media.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security, 11(3): 431-448.

Chang, J. (2013). The Dark Cloud of Convenience: How the HIPAA Omnibus Rules Fail to Protect Electronic Personal Health Information. Loyola of Los Angeles Entertainment Law Review 34(2), 119-154.

Costello, T., & Reback, S. (2014, August). Bloomberg Government. Finance in the Cyber Crosshairs. Retrieved from http://www.multivu.com/players/English/7371431-bloomberg-visa-the-digital-trust-securingcommerce/flexSwf/impAsset/document/65195196-9c27-47d8-8abc-b422a1f90486.pdf

Dane, K. (May 2016). Do Data Breaches Matter? A Review of Breach Data and What to Do Next. ISSA Journal, 22-29.

Dark, M. (2012). Data Breach Disclosure: A Policy Analysis. In I. Management Association (Ed.), Cyber Crime: Concepts, Methodologies, Tools and Applications (pp. 430-456). Hershey, PA: IGI Global. doi:10.4018/978-1-61350-323-2.ch302. Retrieved from https://www.igi-global.com/chapter/data-breach-disclosure/60963?camid=4v1

Dark, M. J. (2011). Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives (pp. 1-306). Hershey, PA: IGI Global. doi:10.4018/978-1-61692-245-0. Retrieved from https://books.google.com/books?hl=en&lr=&id=gRWfToJiWQgC&oi=fnd&pg=PA226&dq=cyber+%2Bdisclosure+%2Beffectiveness+%2Bbreach&ots=i0CY5EYEpO&sig=MRPDYcp-hupRED0dxKY4GOqUW0w#v=onepage&q=cyber%20%20disclosure%20%20effectiveness%20%20breach&f=false

DiLeo, J., & McAlister, L. (2014, April 8). Cyber Chat: Highlights of the SEC's Cybersecurity Roundtable. Heads Up, Volume 21, Issue 9. Deloitte Development LLC. Retrieved from: https://www.iasplus.com/en-us/publications/us/heads-up/2014/sec-cybersecurity

Dorantes, C., & Ko, M. (2006). The impact of information security breaches on financial performance of the breached firms: an empirical investigation. Journal of Information Technology Management, 17(2): 13-22.

Draper, A. (2007). Identity Theft: Plugging the Massive Data Leaks with Stricter Nationwide Breach-Notification Law. John Marshall Law Review, 40(2): 681-702.

Farrow, S. (2016). Cybersecurity: Integrating Information into the Microeconomics of the Consumer and the Firm. Journal of Information Security, 7, 281-290. http://dx.doi.org/10.4236/jis.2016.75023

Farrow, S., & Szanton, J. (2016). Cybersecurity Investment Guidance: Extensions of the Gordon and Loeb Model. Journal of Information Security, 7, 15-28. http://dx.doi.org/10.4236/jis.2016.72002

Faulkner, B. (2007). Hacking into Data Breach Notification Laws. Florida Law Review 59(5), 1097-i. http://heinonline.org/HOL/Page?handle=hein.journals/uflr59&div=40&g_sent=1&collection=journals#

Ferraro, M. F. (2014). 'Groundbreaking' or Broken? An Analysis of SEC Cyber-Security Disclosure Guidance, Its Effectiveness, and Implications. Albany Law Review, 77, 2014, 297-347.

Ferrell, A. (2003). Mandated disclosure and stock returns: Evidence from the over-the-counter market. Harvard Law and Economics Discussion Paper No. 453. http://www.law.harvard.edu/programs/olin_center/papers/pdf/453.pdf

Fisk, G., Ardi, C., Fisk, M., Heidemanny, J., Papadopoulos, C., & Pickett, N. IEEE, 2015 IEEE CS Security and Privacy Workshops. (2015). Privacy Principles for Sharing Cyber Security Data, Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7163225

Gal-Or, E., & Ghose, A. (June 2005). The Economic Incentives for Sharing Security Information. Information Systems Research, 16 (2), 186–208.

Gatzlaff, K. M., & McCullough, K. A. (2010). The Effect of Data Breaches on Shareholder Wealth. Risk Management and Insurance Review, 13: 61-83.

Gelos, R.G., & Wei, S.J. (2002). Transparency and international investor behavior. (Working Paper 9260). Cambridge, MA: National Bureau of Economic Research. https://www.imf.org/external/pubs/ft/wp/2002/wp02174.pdf

Ghose, A. (2006). Information Disclosure and Regulatory Compliance: Economic Issues and Research Directions. Retrieved from https://ssrn.com/abstract=921770 or http://dx.doi.org/10.2139/ssrn.921770

Goel, S., & Shawky, H. A. (2014). "The Impact of Federal and State Notification Laws on Security Breach Announcements," Communications of the Association for Information Systems: Vol. 34 (Article 3): 37-50. http://aisel.aisnet.org/cais/vol34/iss1/3

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing Information on Computer Systems Security: An Economic Analysis. Journal of Accounting and Public Policy, 22 (6): 1-38.

Gordon L.A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006b). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. Journal of Accounting and Public Policy, 25: 503– 30.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. MIS Quarterly, 34(3): 567-A2.

Gordon, L.A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015a). Externalities and the magnitude of cybersecurity underinvestment by private sector firms: a modification of the Gordon-Loeb Model. Journal of Information Security, 6: 24-30.

Gordon, L.A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015b). Increasing cybersecurity investments in private sector firms. Journal of Cybersecurity, 1: 3-17.

Gostin, L., Levit, L., & Nass, S. (Eds). (2009). Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Washington, DC: National Academies Press.

Grant, G., & Grant, T. (2014). SEC Cybersecurity Disclosure Guidance Is Quickly Becoming a Requirement. The CPA Journal. May 2014, 69-71.

Greenstone, M., Oyer, P., & Vissing-Jorgensen, A. (2004). Mandated disclosure, stock returns, and the 1964 Securities Act Amendments. Stanford University, Manuscript. http://faculty.haas.berkeley.edu/vissing/qje.pdf

Gregory, H. J. (2014, June). SEC Review of Disclosure Effectiveness. Practical Law The Journal, 28-31.

Hausken, K. (November–December 2007). Information sharing among firms and cyber attacks. Journal of Accounting and Public Policy, 26(6): 639-688.

Healy, P.M., & Palepu, K.G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. Journal of Accounting and Economics, 31, 405–440.

Heil, R., Kulikova, O., Pieters, W., & van den Berg, J. 2012 International Conference on Cyber Security. (2012). Cyber Crisis Management: A decision-support framework for disclosing security incident information. Retrieved from http://eprints.eemcs.utwente.nl/23955/01/Wolter_Pieters.pdf

Heitzenrater, C., & Simpson, A. (2016). Policy, statistics and questions: Reflections on UK cyber security disclosures. Journal of CyberSecurity. Oxford Academic. Oxford University Press. 2 (1): 43-56.

Hilary, G., Segal, B., & Zhang, M. H. (2016, October). Cyber-Risk Disclosure: Who Cares? (Georgetown McDonough School of Business Research Paper No. 2852519). Retrieved from https://ssrn.com/Abstract/Summary=2852519; http://dx.doi.org/10.2139/ssrn.2852519

Janger, E., & Schwartz, P. (2007). Notification of Data Security Breaches. Michigan Law Review, 105(5): 913-984.

Jin, J. (Fall 2015). Cybersecurity Disclosure Effectiveness on Public Companies (Senior thesis). Retrieved from James Madison University Senior Honors Projects. (Paper 1). http://commons.lib.jmu.edu/honors201019/1

Joerling, J. (2010). Data Breach Notification Laws: An Argument for Comprehensive Federal Law to Protect Consumer Data. Washington University Journal of Law and Policy, 32(1): 467-488.

Karmel, R. S. (2016). Disclosure Reform—The SEC Is Riding Off in Two Directions at Once. Business Lawyer, 71(3): 781-834.

Khansa, L., Bruyaka, O., Cook, D., & James, T. (2012). Impact of HIPAA provisions on the stock market value of healthcare institutions, and information security and other information technology firms, Computers & Security, 31: 750-770.

Koch, D. D. (2017). Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age? Journal of Health Care Finance, 43 (3): 1-32.

Kurt, A. (2015). Effectiveness of Cyber Security Regulations in the US Financial Sector: A Case Study. Master's thesis. Retrieved from Carnegie Mellon University. http://www.contrib.andrew.cmu.edu/~asimk/ResearchThesis.pdf

Kvochko, E., & Pant, R. (2015, March). Why Data Breaches Don't Hurt Stock Prices. Harvard Business Review, https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

Lang, M.H., & Lundholm, R.J. (1996). Corporate disclosure policy and analyst behavior. The Accounting Review, 71, 467–492. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=9611271989&site=ehost-live

Laube, S., & Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. Journal of CyberSecurity. Oxford Academic. Oxford University Press. 2 (1): 29-41.

Lazarus, D. (2013, August 15). CVS thinks $50 is enough reward for giving up healthcare privacy. Los Angeles Times. Retrieved from http://articles.latimes.com/2013/aug/15/business/la-fi-lazarus-20130816

Lenard, T. M., & Rubin, P. H. (2005). An Economic Analysis of Notification Requirements for Data Security Breaches. Emory Law and Economics Research Paper No. 05-12. Retrieved from https://ssrn.com/abstract=765845; http://dx.doi.org/10.2139/ssrn.765845

Leuz, C., & Verrecchia, R.E. (2000). The economic consequences of increased disclosure. Journal of Accounting Research, 38, Issue Supplement, 91–124. Retrieved from: http://faculty.chicagobooth.edu/christian.leuz/research/papers/economic_consequences_of_increased_disclosure.pdf

Leuz, C., & Wysocki, P. (2008). Economic Consequences of Financial Reporting and Disclosure Regulation: A Review and Suggestions for Future Research. Retrieved from https://ssrn.com/abstract=1105398 or http://dx.doi.org/10.2139/ssrn.1105398

Litan, A. (2007, August 20). Use TJX Breach to Improve Protection of Customer Data. Gartner, Inc. Retrieved from https://www.gartner.com/doc/513206/use-tjx-breach-improve-protection

Masterson, J. D. (2015, June 25). Emerging SEC guidance and enforcement regarding data privacy and breach disclosures. Retrieved June 29, 2017, from http://www.insidecounsel.com/2015/06/25/emerging-sec-guidance-and-enforcement-regarding-da

Michael, C. D., Thomas, P.F., & Tucci, A. E. Cyber Risks in the Marine Transportation System. U.S. Coast Guard. Retrieved from http://docplayer.net/23988256-Cyber-risks-in-the-marine-transportation-system-historic-background-and-coast-guard-mission-cyber-risks-and-the-marine-transportation-system.html

Moore, T. Harvard University. (2010). Introducing the Economics of Cybersecurity: Principles and Policy Options. Retrieved from http://cs.brown.edu/courses/csci1800/static/files/documents/SR5-10.pdf

Moriarty, K. M. (November/December 2011). Incident Coordination. IEEE Security & Privacy, 9(6): 71-75.

Mulligan, D. K., & Sedenberg, E. M. (2015). Public Health as a Model for Cybersecurity Information Sharing. Berkeley Technology Law Journal, 30(3): 1687-1739.

Muntermann J., & Roßnagel, H. (2009). On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market. In: Jøsang A., Maseng T.,

Knapskog S.J. (eds) Identity and Privacy in the Internet Age. NordSec 2009. Lecture Notes in Computer Science, vol 5838. Springer, Berlin, Heidelberg. Retrieved from https://link.springer.com/chapter/10.1007/978-3-642-04766-4_1

Parsons, C. (2016). The (In)effectiveness of Voluntarily Produced Transparency Reports. Retrieved from https://ssrn.com/abstract=2798855; http://dx.doi.org/10.2139/ssrn.2798855

Pelliciotta, J. (2017, April 6). Congress Invalidates New FCC Privacy and Data Security Rules. The National Law Review. Retrieved from http://www.natlawreview.com

Peters, R. (2014). So You've Been Notified, Now What: The Problem with Current Data-Breach Notification Laws. Arizona Law Review, 56(4): 1171-1202.

Picanso, K. (2006). Protecting Information Security under Uniform Data Breach Notification Law. Fordham Law Review 75(1): 355-390.

Romanosky, S., Acquisti, A., & Telang, R. (2011). Do data breach disclosure laws reduce identity theft? Journal of Policy Analysis and Management, 30(2), 256-286.

Sarra, J. (2007). Disclosure as Public Policy Instrument in Global Capital Markets. Texas International Law Journal, 42(3): 875-898.

Shackelford, S. (2012). Should your firm invest in cyber risk insurance? Business Horizons, 55(4): 349-356.

Shumsky, T. (2016, September 19). Corporate Judgment Call: When to Disclose You've Been Hacked. The Wall Street Journal. Retrieved from https://www.wsj.com/articles/corporate-judgment-call-when-to-disclose-youve-been-hacked-1474320689

Singer, P., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs To Know. Oxford University Press.

Simon, C.J. (1989). The effect of the 1933 Securities Act on investor information and the performance of new issues. The American Economic Review, 79, 295–318. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=4506297&site=ehost-live

Spanos, G., & Angelis, L. (2016). The Impact of Information Security Events to the Stock Market: A Systematic Literature Review. Computers & Security. P. 216-229.

Stein, S. (2017). Corporate Cyber Risk Disclosures Jump Dramatically in 2017. The Bureau of National Affairs, Inc. Retrieved from https://www.bna.com/corporate-cyber-risk-n73014462313/

Steptoe & Johnson LLP. (2016). Comparison of US States and Federal Security Breach Notification Laws. Retrieved from: http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf

Stewart, B. (2015, April 14). Sarbanes Oxley Compliance - Transparency and Responsibility. Retrieved from https://www.itispivotal.com.

Stigler, G.J. (1964). Public regulation of the securities markets. The Journal of Business, 37, 117–142.

Trope, R. L., & Hughes, S. J. (2011, December). The SEC Staff's 'Cybersecurity Disclosure' Guidance: Will It Help Investors or Cyber-thieves More? Business Law Today, 1-4.

U.S. Chamber of Commerce, Center for Capital Markets Competitiveness (CCMC) (2014, July). Corporate Disclosure Effectiveness: Ensuring a Balanced System that Informs and Protects Investors and Facilitates Capital Formation. Retrieved from http://www.centerforcapitalmarkets.com/wp-content/uploads/2014/07/CCMC_Disclosure_Reform_Final_7-28-20141.pdf

U.S. Congress, Committee on Commerce, Science, and Transportation. (2013, April 9). Senate Commerce Committee (J. D. Rockefeller IV, Author) [Cong. Doc. from 113th Cong., 1st sess.]. Retrieved June 29, 2017, from https://www.commerce.senate.gov/public/_cache/files/49ac989b-bd16-4bbd-8d64-8c15ba0e4e51/B93E89CD80273341701DA31B2B6E1F6A.4-9-13-letter-to-chairman-white.pdf

U.S. Department of Health and Human Services. Breach Notification Rule. (2013, July 26). Retrieved from https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

U.S. Department of Health and Human Services, Office for Civil Rights. Breaches Affecting 500 or More Individuals. (2017, June 15). Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Van Erp, J. (2010), Regulatory Disclosure of Offending Companies in the Dutch Financial Market: Consumer Protection or Enforcement Publicity? Law & Policy, 32: 407-433.

Viswanatha, A., & McMillan, R. (2017, January 23). Yahoo Faces SEC Probe Over Data Breaches; Investigation focuses on whether two massive hacks should have been reported sooner to investors. Wall Street Journal. Retrieved from https://search.proquest.com/news/docview/1861611511?accountid=31567; https://www.wsj.com/articles/yahoo-faces-sec-probe-over-data-breaches-1485133124

Weil, D., Fagotto, E., Fung, A., & Graham, M. (2006). The effectiveness of regulatory disclosure policies. Journal of Policy Analysis and Management, 25(1): 155–181.

Winn, J. (2009). Are 'Better' Security Breach Notification Laws Possible? Berkeley Technology Law Journal, 24, Retrieved from https://ssrn.com/abstract=1416222

Young, S. (2013). Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches. Journal Of Corporation Law, 38(3): 659-679.

Zamorski, M. J. (2005). Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. (FIL-27-2005). Retrieved from Federal Deposit Insurance Corporation website https://www.fdic.gov/news/news/financial/2005/fil2705.html.