Online Appendix

Risk management, firm reputation, and the impact of successful cyberattacks on target firms

May 2019

Appendix A
U.S. Security Breach Notification Laws and Regulations

This appendix summarizes laws and regulations that require publicly listed firms in the U.S. to notify affected individuals about data breaches and report the breaches to state governments and other regulatory agencies. We briefly describe the requirements and developments of these laws and regulations including the State Security Breach Notification Laws, the SEC Cybersecurity Disclosure Guidance, and the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which could affect corporate disclosure decision and thus the coverage of incidents reported by the PRC database.

A.1 State Security Breach Notification Laws

State Security Breach Notification Laws require firms to inform affected state residents about compromise of their personal information. While details of the legislations vary across states, they typically contain several common elements such as entities that are subject to the regulations (e.g., individuals, businesses, and government entities); the definition of personal information (e.g., information that can be used on its own or with other information to identify a person); the definition of breaches (e.g., accessed and/or disclosed in an unauthorized fashion); requirements for notification (e.g., timing/method of notice and entities to be notified); and exemptions (e.g., encrypted personal information). One important note regarding State Security Breach Notification Laws is that disclosure is required based on the residency of the affected consumers, not the actual location of the data breach. The National Conference of State Legislature (NCSL) provides a list of security breach laws.[1]

Appendix Table A summarizes the effective date of the State Security Breach Notification Laws.[2] As of July 2018, all 50 states and Washington D.C., Guam, Puerto Rico, and Virgin Islands in the U.S. have legislated such a law. California legislated such a law in 2003, followed by nine states in 2005 and 18 more in 2006. By 2009, a total of 46 states and four U.S. territories had legislated a law. Alabama and

[1] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[2] https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

South Dakota were the last to adopt the laws in 2018. Thus, the number of states that require data breach notification has increased over our sample period, suggesting that more firms are subject to breach notification requirements.

A.2 SEC Cybersecurity Disclosure Guidance

In addition to the notification requirement by the State Security Breach Notification Laws, publicly traded firms in the U.S. are required to disclose "materially important" cybersecurity risks and cyber incidents according to the Securities and Exchange Commission (SEC) Cybersecurity Disclosure Guidance. However, the SEC 2011 rules have been criticized by lawyers and investors since the disclosure requirements are too general without detailed instruction about the coverage of information, and the definition of "materiality" is vague and thus is subject to alternative interpretations, which may result in underreporting of cybersecurity events by attacked firms.[3] On February 21, 2018, the SEC updated the 2011 guidance regarding disclosure requirements under the federal securities laws and related policies and procedures. To address the negative consequences associated with cybersecurity incidents in a more comprehensive manner, the new SEC guideline now requires the firms to disclose the board's role in overseeing cybersecurity risk management, and prohibits insiders from trading on material nonpublic information relating to cybersecurity risks and incidents.

A.3 HIPAA Privacy Rule

The HIPAA Privacy Rule enacted in 2003 has established national standards to protect privacy regarding certain health information and medical records of individuals that are held by "covered entities" (e.g., health care clearinghouses, employer-sponsored health plans, health insurers, and medical service providers that engage in certain transactions). The Privacy Rule requires covered entities and their business associates, who hold and transmit health information in electronic form, to protect the privacy of personal health information, and sets limits and conditions on the use and disclosure of such information without patient authorization. The rule also requires covered entities and their business associates to notify the Secretary of the U.S. Department of Health and Human Services (HHS) if they discover a breach of unsecured protected health information.[4]

[3] See, for instance, "Senators Ask Wall St. Watchdog to Review Cyber Breach Disclosure Rules," *Reuters* (September 26, 2017). https://www.reuters.com/article/us-usa-cyber-senate/senators-ask-wall-st-watchdog-to-review-cyber-breach-disclosure-rules-idUSKCN1C02WU.

[4] The submitted breaches affecting 500 or more individuals are publicly available at the following website: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Due to the large size of submitted breaches, the HHS has become a major information source of data breaches since the inception of its public disclosure.

Appendix Table A
Effective Dates of Data Breach Legislation Implemented at Each U.S. State and Territory

U.S. State and Territory	Effective date
Alabama	June 1, 2018
Alaska	July 1, 2009
Arizona	December 31, 2006
Arkansas	August 12, 2005
California	July 1, 2003
Colorado	September 1, 2006
Connecticut	January 1, 2006
Delaware	June 28, 2005
District of Columbia	July 1, 2007
Florida	July 1, 2014
Georgia	May 5, 2005
Guam	July 11, 2009
Hawaii	January 1, 2007
Idaho	January 1, 2006
Illinois	June 27, 2006
Indiana	July 1, 2006
Iowa	July 1, 2008
Kansas	January 1, 2007
Kentucky	July 15, 2014
Louisiana	January 1, 2006
Maine	January 31, 2006
Maryland	January 1, 2008
Massachusetts	October 31, 2007
Michigan	July 2, 2007
Minnesota	January 1, 2006
Mississippi	July 1, 2011
Missouri	August 28, 2009
Montana	March 1, 2006
Nebraska	July 14, 2006
Nevada	January 1, 2006
New Hampshire	January 1, 2007
New Jersey	January 1, 2006
New Mexico	January 16, 2017
New York	December 7, 2005
North Carolina	December 1, 2005
North Dakota	June 1, 2005
Ohio	February 17, 2006
Oklahoma	November 1, 2008
Oregon	October 1, 2007
Pennsylvania	June 20, 2006
Puerto Rico	January 5, 2006
Rhode Island	March 1, 2006
South Carolina	July 1, 2009
South Dakota	July 1, 2018
Tennessee	July 1, 2005
Texas	April 1, 2009
Utah	January 1, 2007
Vermont	August 12, 2012
Virgin Islands	October 17, 2005
Virginia	July 1, 2008
Washington	July 24, 2005
West Virginia	June 6, 2008
Wisconsin	March 31, 2006
Wyoming	July 1, 2007

Appendix B
Time Interval from the Occurrence of Cyberattacks to Their Disclosure

This appendix presents summary statistics for the number of days from the date a cyberattack occurred to the date in which the incident is discovered by a firm or a third party and the number of days from the date in which the incident is discovered by a firm or a third party to the date of media reporting (a firm's reporting to the state regulator, a firm's SEC 8-K filing). We manually collect the information on occurrence, discovery, and reporting dates by searching *Factiva*, breach reports disclosed by the state Attorney General's Offices, and cyber security expert blogs such as Krebs on Security (https://krebsonsecurity.com).

Time interval (days)	N	Mean	Median	Min.	Max.
From occurrence of the incidence to discovery	40	47.2	14.5	0	416
From discovery to media reporting	67	16.2	10.0	0	140
From discovery to reporting to the state regulator	35	27.9	18.0	1	135
From discovery to reporting to the SEC	12	19.3	9.0	0	70

Appendix C
Effects of Cyberattacks on the Presence of CIOs and Outside Directors with CIO Experience in the Post-Attack Period

In this appendix, we examine the effect of cyberattacks on the presence of the Chief Information Officer (CIO) and the proportion of outside directors with prior CIO experience to the total number of directors on the board. Attacked firms often announce the replacement of responsible executives such as the CIO to cope with the aftermath of the attack. For instance, Equifax announced the replacements of CIO and Chief Security Officer eight days after its initial public announcement of cybersecurity incident on September 7, 2017. The results reported in Appendix Table C. In column (1), we use an indicator for the presence of the CIO as the dependent variable. We find that the coefficient on the interaction term between *Post* and *Cyberattack* is positive and significant at the 1% level, suggesting that the likelihood of hiring the CIO increases for attacked firms in the post-attack period. The presence of the CIO is particularly evident in the first two years ($Year_{t+2}$) after the attack (column (2)). In columns (7) and (8), we use as the dependent variable the proportion of outside directors with CIO experience on the board and find that it increases significantly in the post-attack period, especially in $Year_{t+2}$, suggesting that attacked firms actively look for board members with IT expertise.

We next investigate whether a firm's decision to invest in risk management policies in the post-attack period is affected by its customer clientele. We divide the sample into firms operating in unique industries and those operating other industries according to industry-median product uniqueness (the ratio of a firm's selling expenses to sales (Titman and Wessels (1988)). We expect customers of firms that sell more unique or specialized products (e.g., Tiffany & Co.) to have greater concerns about data security and thus to demand more investment in cybersecurity. Consistent with this expectation, we find that an increase in cybersecurity investment in the post-attack period measured by the presence of the CIO is concentrated among firms operating in the unique industry (columns (3)-(6)). We also find some weak evidence that the proportion of outside directors with CIO experience increases in $Year_{t+2}$ only among firms operating in the unique industry (columns (9)-(12)). These results suggest that firms' post-attack investment in risk management policies is greater for firm that sell more unique products and thus cater to customers with higher demands for data security.

Appendix Table C
Effects of Cyberattacks on the Presence of CIOs and the Proportion of Outside Directors with CIO Experience on the Board

The table presents estimates of ordinary least squares (OLS) regressions in which the dependent variables are an indicator for the presence of a chief information officer (CIO) in a given year in columns (1)-(6) and the proportion of outside directors with CIO experience to the total number of directors on the board in columns (7)-(12). The sample consists of 1,160 firm-year observations (113 treated firms that experience a cyberattack involving financial information loss over the period 2005 to 2015 and 113 control firms that do not experience a cyberattack over the same period). The propensity score is calculated using the logit regression of *Cyberattack* (an indicator that takes the value of one if a firm experiences a cyberattack involving financial information loss, and zero otherwise) on firm size, stock performance, stock return volatility, leverage, and institutional blockholder (indicator). We require both treated and matching firms to be in the same industry (the same two-digit standard industrial classification (SIC) codes) and in the same fiscal year. *Post* is an indicator that takes the value of one for post-attack period (year *t*, year *t*+1, and year *t*+2), and zero for pre-attack period (year *t*-1 and year *t*-2, and year *t*-3), where year *t* is the fiscal year in which a cyberattack occurs. Columns (3)-(6) and (9)-(12), we divide the sample into two subgroups according to whether firms operate in the unique industry. *Unique industry* is an indicator that takes the value of one if a firm's industry median product uniqueness (selling expense / sales) is above the sample median, and zero otherwise. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

	Presence of the CIO (indicator)						Proportion of outside directors with CIO experience					
	Full sample		Unique industry		Non-unique industry		Full sample		Unique industry		Non-unique industry	
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Post (indicator) ×	0.077***		0.091**		0.061		0.003*		0.003		0.004	
Cyberattack (indicator)	(0.010)		(0.013)		(0.216)		(0.081)		(0.274)		(0.140)	
Year $_t$		0.085*		0.068		0.102		0.000		-0.002		0.002
		(0.061)		(0.236)		(0.168)		(0.920)		(0.414)		(0.164)
Year $_{t+1}$		0.077*		0.103**		0.046		0.003		0.002		0.004
		(0.072)		(0.045)		(0.531)		(0.208)		(0.504)		(0.321)
Year $_{t+2}$		0.033		0.028		0.036		0.009**		0.012**		0.005
Control variables (ROA and those used in Panel B of Table VII)	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y
Firm fixed effects	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Industry-year cohort fixed effects	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Observations	1,160	1,135	650	631	500	495	1,160	1,135	650	631	500	495
Adj. R^2	0.557	0.561	0.615	0.624	0.478	0.470	0.724	0.727	0.730	0.732	0.679	0.685

Appendix D
Effects of Cyberattacks on the Value of Individual Industry Peer Firms

In this appendix, we examine the effects of cyberattacks on the value of individual industry peer firms. Panel A of Appendix Table D shows the CARs for individual peer firms of an attacked firm. We find that the mean individual peer firm CAR (-1, 1) computed using the CRSP value-weighted index return as the market portfolio return is an insignificant -0.03%. However, the median individual peer firm CAR (-1, 1) is -0.18%, which is significant at the 1% level, suggesting that cyberattacks have a significant negative spillover effect on individual industry peer firms. Using the CRSP equally weighted index return as the market portfolio return leads to similar results.

Next, to examine whether spillover effects shown in Panel A differ across characteristics of peer firms, in Panel B of Appendix Table D, we estimate OLS regressions of CARs (-1, 1) for individual peer firms of attacked firms on peer firm characteristics and CARs (-1, 1) for attacked firms. We include as peer firm characteristics an indicator that takes the value one if a peer firm is headquartered within 60 miles of the attacked firm, and zero otherwise (*Within 60 miles of an attacked firm (indicator)*), the correlation between the individual industry peer firm's stock return and the attacked firm's stock return (*Attacked firm CAR (-1, 1)*) for the year preceding the cyberattack announcement (*Return correlation*), and other firm characteristics measured in fiscal year immediate before the cyberattack announcement used in Panel C of Table IV. In Regression (1), we find that the coefficient on the *Attacked firm CAR (-1, 1)* is positive and significant at the 5% level, suggesting that cyberattacks signal negative information about industry-wide problems in risk management and IT security systems. For peer firm characteristics, we find that the coefficient on *Within 60 miles of an attacked firm (indicator)* and *Return correlation* are negative but insignificant. However, the coefficients on *ROA* and *Sales growth* are positive and significant, suggesting that cyberattacks affect better-performing peer firms less adversely. The coefficients on Tobin's *q* is negative and significant at the 10% level, suggesting that peer firms with higher future growth opportunities suffer more from focal firms' cyberattacks. In Regression (2), we include an interaction term between *Attacked firm CAR (-1, 1)* and *Within 60 miles of an attacked firm (indicator)* as an additional explanatory variable. We find that while the coefficient on *Within 60 miles of an attacked firm (indicator)* remains negative and insignificant, its interaction with *Attacked firm CAR (-1, 1)* is negative and significant at the 5% level. These results indicate that geographically proximate peer firms benefits from cyberattcks on the other firms in the same industry, possibly due to the weakening industry position of an attacked firm in the local area. In Regression (3), we add *Risk committee (indicator)*, *Presence of CIO (indicator)*, and governance characteristics (i.e., board size, proportion of independent directors on the board, and CEO-chair duality (indicator)) as additional explanatory variables. We find that the coefficient on the proportion of outside directors on the board is positive and significant,

suggesting that well-governed peer firms suffer less from their rivals' cyberattacks. However, the coefficient on other variables are not significant.

Overall, these results suggest that although cyberattacks, on average, negatively affect industry peer firms' market values, some peer firms such as well-performing firms, high-growth firms, firms with more outside directors, and firms that are located proximately to the attacked firm are affected less adversely by cyberattacks in their industry.

Appendix Table D
Effects of Cyberattacks on the Value of Individual Industry Peer Firms

The table presents the mean and median cumulative abnormal returns (CARs) for 6,094 individual industry peer firms of an attacked firms (Panel A) and estimates of ordinary least squares (OLS) regressions in which the dependent variable is the CAR from one day before the attack announcement date to one day after the attack announcement date (CAR (-1, 1)) for individual industry peer firms. The sample consists of 5,775 individual industry peer firms that have the same four-digit SIC code as firms experiencing cyberattacks over the period 2005 to 2017. *Within 60-miles of an attacked firm* is an indicator that takes the value one if an industry peer firm is located within 60-miles of the attacked firm, and zero otherwise. *Returns correlation* is the correlation between the individual industry peer firm return and the attacked firm return for the year preceding the cyberattack announcement. The market model parameters are estimated using 220 trading days of return data beginning 280 days before and ending 61 days before the breach announcements, using the CRSP value-weighted return as a proxy for the market portfolio return. In Panel A, the numbers in parentheses are *p*-values for *t*-tests and *z*-values for Wilcoxon signed-rank tests that the mean CAR and the median CAR are equal to zero. In Panel B, *p*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustered at the event level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A. CARs for individual industry peer firms

	CRSP value-weighted index return		CRSP equally weighted index return	
CARs (%)	Mean	Median	Mean	Median
CAR (-1, 1)	-0.034	-0.177***	-0.071	-0.169***
	(0.522)	(-3.456)	(0.176)	(-3.867)
CAR (-2, 2)	0.062	-0.213**	-0.008	-0.261***
	(0.370)	(-2.538)	(0.907)	(-3.288)
CAR (-5, 5)	0.266	-0.237	-0.157	-0.295***
	(0.018)	(-1.477)	(0.163)	(-4.106)

Panel B. OLS regressions of CARs (-1, 1) for individual industry peer firms

	CAR (-1, 1)		
Independent variable	(1)	(2)	(3)
Attacked firm CAR (-1, 1): a	0.125**	0.138***	0.133***
	(0.017)	(0.006)	(0.009)
Within 60 miles of an attacked firm (indicator): b	-0.000	-0.002	-0.002
	(0.979)	(0.446)	(0.457)
a × b		-0.230**	-0.211**
		(0.023)	(0.030)
Returns correlation	-0.008	-0.007	-0.008
	(0.181)	(0.200)	(0.153)
Firm size	0.000	0.000	0.000
	(0.565)	(0.594)	(0.545)
Log (firm age)	-0.001	-0.001	-0.001
	(0.345)	(0.385)	(0.303)
ROA	0.011**	0.011**	0.010
	(0.031)	(0.027)	(0.101)
Leverage	0.000	0.000	0.000
	(0.927)	(0.931)	(0.939)
Financially constraint (indicator)	0.001	0.001	0.001
	(0.744)	(0.734)	(0.699)
Sales growth	0.005*	0.005*	0.005*
	(0.095)	(0.088)	(0.067)
Tobin's *q*	-0.001*	-0.001*	-0.001*
	(0.079)	(0.066)	(0.098)
Institutional block ownership	-0.000	-0.000	-0.000
	(0.934)	(0.917)	(0.880)
Risk committee (indicator)			-0.002
			(0.470)
Board size			-0.000
			(0.516)
Proportion of outside directors on the board			0.013**
			(0.041)
CEO-chair duality (indicator)			-0.000
			(0.817)
Year fixed effects	Y	Y	Y
Industry fixed effects	Y	Y	Y
Observations	5,775	5,775	5,601
Adj. R^2	0.024	0.025	0.026