International Journal of Services and Standards

ISSN online: 1740-8857 - ISSN print: 1740-8849
https://www.inderscience.com/ijss

The effects of the legal environment on cybersecurity

Kam C. Chan, Barbara Farrell, Patricia Healy, Maria Tan

DOI: 10.1504/IJSS.2022.10047146

Article History:

Received:	03 March 2021
Accepted:	25 November 2021
Published online:	09 August 2023

The effects of the legal environment on cybersecurity

Kam C. Chan*, Barbara Farrell, Patricia Healy and Maria Tan

Lubin School of Business,
Pace University,
Pleasantville, NY, 10570, USA
Email: kchan@pace.edu
Email: bfarrell@pace.edu
Email: phealy@pace.edu
Email: marichris.tan@gmail.com
*Corresponding author

Abstract: Cybersecurity failure poses a risk to all firms. Cyber attackers exploit vulnerabilities to steal assets and information, jeopardising the victim's ability to deliver products or services. Understanding the ways to strengthen cybersecurity can help mitigate the risk of cybersecurity failures. Examining the effects of a country's legal environment on cybersecurity, this study finds that the strength of cybersecurity is positively associated with the strength of laws in place and the extent of legal enforcement. In addition, we observe stronger cybersecurity in countries with more resources and higher percentages of internet users. This study helps regulators understand the factors affecting cybersecurity. Analysing factors determining cybersecurity allows investors to predict and assess international differences in cybersecurity risks.

Keywords: cybersecurity; legal environment; rule of law; shareholder rights; GDPR.

Reference to this paper should be made as follows: Chan, K.C., Farrell, B., Healy, P. and Tan, M. (2023) 'The effects of the legal environment on cybersecurity', *Int. J. Services and Standards*, Vol. 13, Nos. 3/4, pp.147–159.

Biographical notes: Kam C. Chan is a Distinguished Professor and Schaeberle Professor of Accounting at Pace University. He joined Pace in 1997 and has received the Kenan Award for Teaching Excellence in 2014. He has published in premier research journals such as *Accounting, Organizations, and Society*, *Auditing: A Journal of Practice and Theory*, *Journal of Accounting and Economics*, *Journal of Business Finance and Accounting*, and *Journal of International Accounting Research*. His research has been abstracted, reprinted, and highly cited by others, including the Securities and Exchange Commission. He received the Outstanding Reviewer Award from the Emerald Literati Network in 2016.

Barbara Farrell is a Professor of Accounting. She is a CPA who has spent time in the Big 8 public accounting and private industry as a Chief Audit Executive. She received Pace's Kenan Award of Teaching Excellence in 2011. She is a member of the Audit Committee of the Board of Trustees at Pace and a member of the Board of Trustees of Academic Federal Credit Union. She also chairs the annual campaign to raise significant donations for student scholarships. She has published in many journals such as *Auditing: A Journal of Practice and Theory* and *CPA Journal*.

Patricia Healy is an Associate Professor of Accounting and was the Undergraduate Program Chair for the Accounting Department. Professor Healy is a CPA and CMA, and she is an active member of the AICPA, AAA, and IMA. She serves on the Accounting Advisory Board for Westchester Community College. Professor Healy was recognised as an outstanding teacher with the Kenan Teaching Award and her strong service to Lubin with the Accounting Department Service award. Professor Healy has published papers on international auditing standards, managing quality control costs, diversity issues in business, implementing the Balanced Scorecard, and governmental accounting issues.

Maria Tan is an Audit Associate at PwC in the Consumer Products sector. She has a BBA and MBA in accounting from Pace University. She has obtained a CPA certificate.

1 Introduction

In the past few decades, e-commerce has dramatically expanded (Wen et al., 2015; Migdadi and Omary, 2017; Isaac et al., 2018; Mohamed and Marthandan, 2019). Along with expanding use of data analytics in business, data protection against e-commerce risks is emerging as a critical issue (Moffitt and Vasarhelyi, 2013; Huerta and Jensen, 2017). Numerous cases of serious cybersecurity breaches with dreadful consequences have occurred in recent years.

Cybersecurity breaches can result in substantial losses for firms and the economy. Colonial Pipeline lost 100 gigabytes of data to hackers in just 2 h on May 6, 2021. The $5,000,000 ransom was just a fraction of the overall damages to the company and the economy. The company's pipeline system was shut down for days, causing a temporary gasoline shortage in some local markets (Reuters, 2021). The short-term fuel shortages and unwanted media attention caused additional stress for the company. Other sufferings include depressed stock prices and higher audit fees subsequent to cybersecurity failures (Telang and Wattal, 2007; Yen et al., 2018; Smith et al., 2019). Moreover, hackers stole 885 million customer records from First American Financial Corporation as well as 540 million customer records from Facebook (Audit Analytics 2020). According to Janjarasjit and Chan (2021), such cybersecurity breaches cause significant emotional distress to information system users.

Responding to rising importance of cybersecurity in the global economy, this study examines the effects of a country's legal environment on the strength of cybersecurity. Cybersecurity is a comprehensive concept encompassing user privacy protection, financial data protection, and operational protection of government and business. Understanding the factors affecting international differences in cybersecurity is essential for regulators seeking to improve cybersecurity. In a globally integrated economy, an analysis of country-level factors affecting cybersecurity could allow managers and investors to assess the cybersecurity risk of firms operating in different countries.

The legal environment presents a new perspective of cybersecurity research. International and national legislative and prosecution efforts have sprung up in response to intensifying cybersecurity risks. The European Union (EU), for instance, passed the General Data Protection Regulation (GDPR) in 2016 to protect the privacy and security

of personal data. Many international firms, including those transacting with EU customers or processing personal data of EU residents, are subjected to GDPR. The US has stepped up prosecuting violators of Rule 30(a) of Regulation S-P, also known as the Safeguards Rule, which is designed to protect confidential customer information (SEC, 2021). Moreover, finding cybersecurity disclosures of Canadian firms to be limited in quality and quantity, Héroux and Fortin (2020) suggest introducing more stringent cybersecurity disclosure regulations. Our study provides a timely assessment of the effects of cybersecurity-related legislative and enforcement efforts.

We update the cybersecurity literature with a larger and more recent dataset. From a sample of 157 countries, this study finds that a country's cybersecurity is positively related to the strength of its legal environment, the size of its economies, and the number of internet users. Specifically, countries with stronger laws and legal enforcement are associated with more robust cybersecurity.

Since firms generally underinvest in cybersecurity (Garcia and Horowitz, 2007; Zhuang et al., 2020), governments have a role in compensating for such underinvestment. The findings of this paper support the notion that government regulation is critical in strengthening cybersecurity practices. In particular, raising the quality of laws and legal enforcement can help strengthen cybersecurity.

The rest of this paper is organised as follows. Section 2 summarises the related literature. Section 3 describes the data and research design. Section 4 reports and discusses the results. Concluding remarks are provided in Section 5.

2 Related literature

2.1 Costs of weak cybersecurity

Cybersecurity breaches induce significant economic impacts on firms. Victims of cybersecurity breaches pay higher audit fees afterward (Yen et al., 2018; Smith et al., 2019; Li et al., 2020). Such higher audit fees compensate for increased audit effort due to cybersecurity risks and information system weaknesses (Rosati et al., 2020). From a sample of 329 firms with cybersecurity breaches, Rosati et al. (2020) observe a significant decrease in the amount of abnormal discretionary accruals and accounting restatements in the two years following cybersecurity breaches, reflecting increased auditor efforts. Telang and Wattal (2007) find that information security software vendors suffer significant drops in stock prices when users of such software are breached. These studies show that information systems exposing company and customer data to cybersecurity risks are costly in many ways.

2.2 National variations

Countries adopt different approaches in regulating and promoting cybersecurity. Renaud et al. (2020) identify a maximum intervention approach and a hands-off approach in managing cybersecurity risk. Jamal et al. (2005) report that the US and the UK followed different approaches in online privacy regulations with the UK focusing on formal government regulations, while the US relying mainly on industry self-regulation and voluntary compliance. Kharlamov and Pogrebna (2021) relate national differences in cybersecurity regulation to differences in human values, such as social embeddedness,

affective values, and individual-based vs. collective-based social values. Implicitly, some countries may need stronger regulations when their citizens take more risks in cyber activities.

National differences can explain the firm's cyber decisions. Examining the early adoption of the US SEC's (Securities and Exchange Commission) eXtensible Business Reporting Language (XBRL) filing requirement, Boritz and Timoshenko (2015) find that US-listed foreign firms were less likely to adopt XBRL than domestic US firms. Investigating the risks of security breaches in offshoring information services, Hahn et al. (2009) find that firms prefer offshore locations with similar political and economic risk environments as the home country. In addition, WhatsApp announced in January 2021 that it would share user information with Facebook, but the new arrangement excludes EU and UK users, presumably due to concerns about GDPR (Taylor, 2021). This study focuses on how cybersecurity is affected by a specific dimension of national characteristics, namely the legal environment.

2.3 Legal environment

La Porta et al. (1998, 2008) suggest that the legal environment significantly impacts minority shareholder protection. Leuz et al. (2003), Fan et al. (2012), Behn et al. (2013), Rahman and Debreceny (2014), and Srinivasan et al. (2015) report consistent evidence that the legal environment affects corporate reporting, financing, and operating activities. We aim to extend this stream of literature by examining how the legal environment and minority shareholder protection affect a country's cybersecurity.

Firms generally underinvest in cybersecurity because of information asymmetry, the free-rider problem, and cybersecurity's meager contribution to corporate revenue (Garcia and Horowitz, 2007; Zhuang et al., 2020). For instance, only 33% of international executives in EY's (2018) survey indicate that their firms have plans to comply with GDPR. Since cybersecurity regulation is a partnership between the private sector and the government (Hooker and Pill, 2016; Eichensehr, 2017), increasing government regulation is often considered necessary to avoid market failure driven by the private sector's underinvestment in cybersecurity (Garcia and Horowitz, 2007; Kirkpatrick, 2019; Zukis, 2020). Countries with stronger legal environments are more likely to

a adopt stringent government regulations and processes to safeguard the internet user's privacy

b impose stronger cybersecurity disclosure requirements to allow shareholders to assess firm risk and monitor firm activities.

An example of such cybersecurity disclosure requirements is the US SEC's cybersecurity guidance of 2018, which requires firms to report cybersecurity incidents and internal control effectiveness on cybersecurity.

The strength of the legal environment depends on two aspects of the regulation (Durnev and Kim, 2005). The *de jure* aspect is the strength of laws in place, while the *de facto* aspect is the strength of legal enforcement. Factor analysis identifies minority shareholder protection (an accepted proxy for the strength of law) and legal enforcement as two underlying aspects of the strength of legal environment (Chan et al., 2017). In other words, the strength of the legal environment is a function of the legal rules in effect and the extent that these rules are being enforced.

Enforcement varies across nations, even when they adopt the same laws. GDPR is a typical example. Enforcement of GDPR is handled directly by each EU country. The French authority fined Google €50 million for failure to adequately disclose how user data is collected and used (Satariano, 2019). Germany imposed its first GDPR penalty of €20,000 on a social media company for data breaches involving user email addresses and personal data (Sutton, 2019). Moreover, investment companies with poor cybersecurity practices are subjected to fines in the US. For example, the SEC fined eight investment companies in 2021 for failing to maintain proper company policies on cybersecurity and inform customers of cybersecurity breaches (SEC, 2021). H1 and H2 consider the *de jure* vs. *de facto* aspects of the legal environment.

H1: The strength of cybersecurity is positively associated with the strength of laws.

H2: The strength of cybersecurity is positively associated with the strength of legal enforcement.

3 Data and research design

With a larger and more recent sample, this study examines how the legal environment of a country affects its strength of cybersecurity. The following paragraphs describe the major variables and their sources.

In this study, the strength of cybersecurity, CYBERSECURITY, is proxied by Global Cybersecurity Index (GCI). GCI is published by International Telecommunication Union (ITU), an agency of the United Nations, to promote information and communication technologies. ITU collects country-level data on cybersecurity through a survey. A panel of experts then reviews the data and determines the GCI component scores for each country. The first two editions of GCI were published in 2015 and in 2017. The 2018 edition, based on a substantially revised methodology, was released in 2019. Kharlamov and Pogrebna's (2021) data contains 74 countries from the 2017 edition of GCI. This study extends the literature by adopting the 2018 edition of GCI, which provides a more updated and much-expanded sample.

The GCI score of each country is a function of five components: the legal framework, technical framework, national policy, research and training, and cooperative partnerships for managing cybersecurity. The legal component represents the presence or absence of specific legislation on data protection, breach notification, identity theft and privacy protection, illegal access, and online harassment. Notice that the strength of laws and strength of legal enforcement highlighted in the hypotheses are broader measures of the legal environment not captured by the GCI score.

Consistent with the prior literature, the strength of laws in place, LAW, is proxied by the World Bank's minority investor protection ranking. Based on Djankov et al.'s (2008) anti-self-dealing index, the minority investor protection ranking boasts a theoretical improvement over La Porta et al.'s (1998) anti-director rights index as a proxy of the strength of laws.

The extent of legal enforcement, ENFORCE, is proxied by Transparency International's Corruption Perceptions Index, which is based on a survey of experts' and business executives' perception of public sector corruption in 180 countries (Behn et al., 2013; Fan et al., 2012). Updated annually and publicly available, the Corruption

Perception index reflects the extent of legal enforcement and is highly correlated with other measures of legal enforcement used in the literature (Chan et al., 2017).

Gross domestic product, GDP, and the percentage of internet users relative to population, USERS, are collected from the World Bank. GDP and USERS are adopted as control variables in the model because financial development, size of economy, and information technology are related (Zagorchev et al., 2011).

The following regression model examines the relationship between GCI and the legal environment.

$$\text{CYBERSECURITY} = \beta_0 + \beta_1\text{ENFORCE} + \beta_2\text{LAW} + \beta_3\text{GDP} + \beta_4\text{USERS} + e$$

where

CYBERSECURITY =GCI score

ENFORCE =181 – Corruption perception index ranking

LAW =191 – Protecting minority investors indicator ranking

GDP =natural logarithm of gross domestic product

USERS =internet users as a percentage of population.

CYBERSECURITY, LAW, ENFORCE, GDP, and USERS are available for 157 countries, which form the final sample. Table 1 reports the summary statistics of the dependent and independent variables. CYBERSECURITY ranges from 0.004 to 0.931, with an average of 0.4837. UK and US earn the two highest scores of 0.931 and 0.926.

Table 1 Summary statistics (sample size =157)

	Mean	*Median*	*Minimum*	*Maximum*
CYBERSECURITY	0.4837	0.4850	0.0040	0.931
ENFORCE	93.14	92	1	180
LAW	105.84	108	1	190
GDP	24.79	24.64	20.03	30.65
USERS	53.50	58.76	2	100
COMMON	0.1847	0	0	1
CIVIL	0.5031	1	0	1

CYBERSECURITY = Global Cybersecurity Index score
ENFORCE = 181 – Corruption Perception Index ranking
LAW = 191 – Protecting Minority Investor ranking
GDP = natural logarithm of gross domestic product
USERS = internet users as a percentage of population
COMMON = 1 for common law origin; 0 otherwise
CIVIL = 1 for civil law origin; 0 otherwise.

The average LAW in the sample is 105.84, with rankings from 1 to 190. To streamline discussion, we apply a transformation to LAW so that a positive sign of its coefficient estimate suggests a positive relationship with CYBERSECURITY. This transformed value is obtained by adding 1 to 190 and then subtracting the old value.

ENFORCE ranges from 1 to 180, with an average of 93.14. ENFORCE is similarly transformed by adding 1 to 180 and then subtracting the old value. The average GDP is 24.79. The average USERS is 53.5% highlighting the importance of cyber transactions and cybersecurity.

Legal origin variables (i.e., COMMON and CIVIL) are used in the supplementary analysis. We follow La Porta et al.'s (1998) legal origin classification, turning to Wikipedia's classification only when the country is missing from La Porta (1998). Common law and civil law are practiced respectively in about 18% and 50% of sample countries. The legal origins of the remaining countries are either religious, mixed, or undetermined.

4 Results

4.1 Main results

Table 2 reports the Pearson correlations among the variables. CYBERSECURITY is positively correlated with other variables. Signs of significant collinearity among the independent variables are not observed.

Table 2 Pearson correlations among variables

	ENFORCE	*LAW*	*GDP*	*USERS*	*COMMON*	*CIVIL*
CYBERSECURITY	0.64223 < 0.0001	0.63809 < 0.0001	0.72514 < 0.0001	0.70785 < 0.0001	0.11450 0.1533	0.23455 0.0031
ENFORCE		0.43842 < 0.0001	0.36695 < 0.0001	0.74365 < 0.0001	0.12808 0.1099	0.11899 0.1377
LAW			0.43679 < 0.0001	0.52067 < 0.0001	0.23077 0.0036	0.02778 0.7298
GDP				0.53185 < 0.0001	0.14949 0.0617	0.26361 0.0009
USERS					0.01544 0.8478	0.22260 0.0051
COMMON						–0.47903 < 0.0001

Table 3 presents the results of the regression analysis. In Model 1, ENFORCE and LAW, carrying significant coefficient estimates of 0.0026 and 0.0025, support the predicted positive association with CYBERSECURITY. Model 2 includes the GDP and USERS variables to control for differences in economy size and internet usage among sample countries. ENFORCE and LAW continue to carry significant positive coefficient estimates in Model 2. The positive and significant coefficients of GDP (0.0626) and USERS (0.0015) underscore the contribution of economic and internet activities to cybersecurity. Model 3 considers the interaction effect of the two dimensions of the legal environment, LAW and ENFORCE, as suggested by Durnev and Kim (2005). The interaction term LEGAL_ENIVORNMENT carries a positive coefficient estimate, which supports the expected positive relationship between cybersecurity strength and the legal

environment. Because including the interaction term and the primary variables (i.e., LAW and ENFORCE) in Model 3 causes collinearity problem, we exclude such results.

Table 3 Summary of regression results (Dependent variable = CYBERSECURITY; Sample size = 157)

Variables	*Model 1*	*Model 2*	*Model 3*
Intercept	–0.0240	–1.4451***	–1.3113***
ENFORCE	0.0026***	0.0015***	
LAW	0.0025***	0.0014***	
LEGAL_ENIVORNMENT			0.0001***
GDP		0.0626***	0.0620***
USERS		0.0015**	0.0022***
F-statistics	101.99***	115.84***	137.59***
Adjusted R^2	0.5642	0.7465	0.7243

LEGAL_ENIVORNMENT = ENFORCE * LAW.

*, **, *** are statistically significant at 10%, 5%, and 1%, respectively.

4.2 Supplementary analysis

The growing importance of cybersecurity has led to corporate governance reforms on cybersecurity in the private sector. The board of directors is responsible for overseeing cybersecurity risk management in firms (Aguilar, 2014). In recent years, shareholders have sued companies for drops in stock prices pursuant to cybersecurity breaches (Nash, 2019), urged the board of directors to adopt strong cybersecurity measures, advocated tying management compensation to cybersecurity performance (Butler, 2019), and pressured firms to strengthen the cybersecurity expertise of corporate board members and employees (Wang, 2019).

According to La Porta et al. (2008), legal origin causes significant legal, economic, and social consequences. Chan et al. (2020) relate a firm's environmental performance to the legal origin and legal enforcement quality of its home country. Common law countries are expected to focus more strongly on protecting minority shareholder value than civil law countries (La Porta et al., 1998; Kock and Min, 2016; Kim et al., 2017), but Spamann's (2009) results based on updated data do not support such expectation.

Table 4 presents supplementary analysis involving legal origin variables. In Models 4, 5, and 6, we examine whether common law countries which emphasise minority shareholder protection are likely to reinforce the shareholder's demand for cybersecurity-enhancing corporate governance and push firms to correct their underinvestment in cybersecurity.

In Model 4, while COMMON's coefficient estimate is insignificant, CIVIL's significant coefficient of 0.1177 suggests higher cybersecurity in civil law countries. However, coefficient estimates of both COMMON and CIVIL are insignificant when GDP and USERS are added as control variables, which is consistent with Spamann's (2009) observation. ENFORCE and RIGHT in Models 4 and 5 and their interaction term LEGAL_ENIVORNMENT in Model 6 all maintain positive significant coefficients. Overall, Table 4 suggests that laws and enforcement are more important factors than legal

origins. The variance inflation factors at about three or less in regressions reported in Tables 3 and 4 are below the general rule of thumb of 10, which quenches collinearity concerns (Marquaridt, 1970).

Table 4 Summary of regression results with legal origins (Dependent variable = CYBERSECURITY; Sample size = 157)

Variables	*Model 4*	*Model 5*	*Model 6*
Intercept	–0.0722*	–1.4402***	–1.3028***
ENFORCE	0.0024***	0.0015***	
LAW	0.0024***	0.0015***	
LEGAL_ENIVORNMENT			0.0001***
COMMON	0.0422	–0.0241	–0.0165
CIVIL	0.1177***	0.0215	0.0159
GDP		0.0620***	0.0616***
USERS		0.0013*	0.0021***
F-statistics	57.22***	77.53***	82.15***
Adjusted R^2	0.5904	0.7464	0.7223

*, **, *** are statistically significant at 10%, 5%, and 1%, respectively.

4.3 Sensitivity analysis

We have conducted the following sensitivity analyses. First, an alternative model with each country's GCI ranking as the dependent variable produces results consistent with those already reported. Second, controlling for national differences by including EU (European Union) membership as a control variable does not materially change our results. Third, we control for industry compositions with data collected from the World Bank in an alternative model, but the new results are not qualitatively different from those already reported. None of the industry variables is statistically significant.

5 Conclusions and future research

In this study, the GCI score proxies for the strength of cybersecurity. Using a sample of 157 countries, this study finds that cybersecurity is positively related to the strength of a country's legal environment, the size of its economies, and the number of internet users. Specifically, countries with a more robust legal environment (i.e., stronger rule of law and legal enforcement) earn higher GCI scores. Cybersecurity is found to be more robust in countries with more resources and more internet activities.

This study extends the literature on the effects of the legal environment on firms and countries. Prior studies have found that the legal environment affects national differences in financial reporting quality of firms and environmental performance. This study shows that the legal environment also affects the strength of cybersecurity among countries.

Serious consequences of the recent cybersecurity breach at Colonial Pipeline draw attention to the need for the private sector to strengthen its cybersecurity (Natter, 2021). As a result, there is a renewed call for more cybersecurity legislation in US. This study

contributes to the literature on the debate between government regulation vs. company self-regulation on cybersecurity. The findings suggest that government intervention in the form of strict rules and effective legal enforcement plays a vital role in promoting cybersecurity.

Future studies can extend the literature in several ways. First, researchers can examine how new cybersecurity regulations such as GDPR affect corporate cybersecurity reforms, user behaviours, and hacking activities. Second, as e-commerce continues to grow rapidly, researchers can investigate how e-commerce growth drives the demand for more government regulation and the firm's cybersecurity initiatives. Third, overall GCI scores are used in this study because the individual component scores are not publicly available. When fine-grained data on cybersecurity becomes available, future studies can separately examine factors determining each aspect of cybersecurity. Fourth, corporate governance reforms can boost the demand for training and certifications of cybersecurity professionals and stimulate cooperation between the government and private sector on cybersecurity issues. As firms start to correct their underinvestment in cybersecurity, future studies may investigate how the strength of cybersecurity, the level of corporate investment in cybersecurity, and the legal environment are interrelated. Fifth, the 2018 edition of GCI was the most current when we collected data for this study. ITU has recently released the 2021 edition of GCI. The Pearson and Spearman correlations between the 2018 and 2021 GCI scores are about 94%. Changes in GCI data have been few and minor, suggesting that cybersecurity doesn't change in a short period. Thus, we do not analyse changes in GCI scores, leaving it as a longitudinal research topic for future researchers.

References

Aguilar, L. (2014) *Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus*, SEC Emblem, 10 June, https://www.sec.gov/news/speech/2014-spch061014laa

Audit Analytics (2020) *Trends in Cybersecurity Breach Disclosures*, https://blog.auditanalytics.com/trends-in-cybersecurity-breach-disclosures-2/

Behn, B.K., Gotti, G., Herrmann, D. and Kang, T. (2013) 'Classification shifting in an international setting: investor protection and financial analysts monitoring', *Journal of International Accounting Research*, Vol. 12, No. 2, pp.27–50.

Boritz, J.E. and Timoshenko, L.M. (2015) 'Firm-specific characteristics of the participants in the SEC's XBRL voluntary filing program', *Journal of Information Systems*, Vol. 29, No. 1, pp.9–36.

Butler, A.M. (2019) *Shareholder Proposals: The New Battleground in Managing Cyber-Risk?*, Intelligize, 5 February, https://www.intelligize.com/shareholder-proposals-the-new-battleground-in-managing-cyber-risk/

Chan, K.C., Hussein, M.E., Seow, G.S. and Tam, K. (2020) 'Corporate environmental performance, legal origin, and investor protection', *Interdisciplinary Environmental Review*, Vol. 20, Nos. 3–4, pp.234–254.

Chan, K., Farrell, B., Healy, P. and Wong, A. (2017) 'Shareholder rights and legal enforcement', *American Journal of Business Research*, Vol. 9, No. 1, pp.73–84.

Djankov, S., La Porta, R., Lopez-de-silanes, F. and Shleifer, A. (2008) 'The law and economics of self-dealing', *Journal of Financial Economics*, Vol. 88, No. 3, pp.430–465.

Durnev, A. and Kim, E.H. (2005) 'To steal or not to steal: firm attributes, legal environment, and valuation', *Journal of Finance*, Vol. 60, No. 3, pp.1461–1493.

Eichensehr, K.E. (2017) 'Public-private cybersecurity', *Texas Law Review*, Vol. 95, No. 3, pp.467–538.

EY (2018) *Global Forensic Data Analytics Survey 2018, How can you Disrupt Risk in an Era of Digital Transformation?*, https://www.ey.com/en_us/assurance/how-to-disrupt-risk-in-an-era-of-digital-transformation

Fan, J.P.H., Titman, S. and Twite, G. (2012) 'An international comparison of capital structure and debt maturity choices', *Journal of Financial and Quantitative Analysis*, Vol. 47, No. 1, pp.23–56.

Garcia, A. and Horowitz, B. (2007) 'The potential for underinvestment in internet security: implications for regulatory policy', *Journal of Regulatory Economics*, Vol. 31, No. 1, pp.37–55.

Hahn, E.D., Doh, J.P. and Bunyaratavej, K. (2009) 'The evolution of risk in information systems offshoring: the impact of home country risk, firm learning, and competitive dynamics', *MIS Quarterly*, Vol. 33, No. 3, pp.597–616.

Héroux, S. and Fortin, A. (2020) 'Cybersecurity disclosure by the companies on the S & P/TSX 60 index', *Accounting Perspectives*, Vol. 19, No. 2, pp.73–100.

Hooker, M. and Pill, J. (2016) 'You've been hacked, and now you're being sued: the developing world of cybersecurity litigation', *Florida Bar Journal*, Vol. 90, No. 7, pp.30–40.

Huerta, E. and Jensen, S. (2017) 'An accounting information systems perspective on data analytics and big data', *Journal of Information Systems*, Vol. 31, No. 3, pp.101–114.

Isaac, O., Mutahar, A.M., Daud, N.M., Ramayah, T. and Aldholay, A.H. (2018) 'The effect of awareness and perceived risk on the technology acceptance model (TAM): mobile banking in Yemen', *International Journal of Services and Standards*, Vol. 12, No. 2, pp.180–204.

Jamal, K., Maier, M. and Sunder, S. (2005) 'Enforced standards vs. evolution by general acceptance: a comparative study of E-commerce privacy disclosure and practice in the United States and the United Kingdom', *Journal of Accounting Research (Wiley-Blackwell)*, Vol. 43, No. 1, pp.73–96.

Janjarasjit, S. and Chan, S.H. (2021) 'Reaction of users as potential victims of information security breach', *Information and Computer Security*, Vol. 29, No. 1, pp.187–206.

Kharlamov, A. and Pogrebna, G. (2021) 'Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity', *Regulation and Governance*, forthcoming, https://doi.org/10.1111/rego.12281

Kim, H., Park, K. and Ryu, D. (2017) 'Corporate environmental responsibility: a legal origins perspective', *Journal of Business Ethics*, Vol. 140, No. 3, pp.381–402.

Kirkpatrick, K. (2019) 'Regulating information technology: why isn't IT regulated, when it can have such substantial impacts on people's lives?', *Communications of the ACM*, Vol. 62, No. 12, pp.19–21.

Kock, C.J. and Min, B.S. (2016) 'Legal origins, corporate governance, and environmental outcomes', *Journal of Business Ethics*, Vol. 138, No. 3, pp.507–524.

La Porta, R., Lopez-de-Silanes, F., Shleifer, A. and Vishny, R.W. (1998) 'Law and finance', *Journal of Political Economy*, Vol. 106, No. 6, pp.1113–1155.

La Porta, R., Silanes, F.L.D. and Schleifer, A. (2008) 'Economic consequences of legal origins', *Journal of Economic Literature*, Vol. 46, No. 2, pp.285–332.

Leuz, C., Nanda, D. and Wysocki, P.D. (2003) 'Earnings management and investor protection: an international comparison', *Journal of Financial Economics*, Vol. 69, No. 3, pp.505–527.

Li, H., No, W.G. and Boritz, J.E. (2020) 'Are external auditors concerned about cyber incidents? Evidence from audit fees', *Auditing: A Journal of Practice and Theory*, Vol. 39, No. 1, pp.151–171.

Marquaridt, D.W. (1970) 'Generalized inverses, ridge regression, biased linear estimation, and nonlinear estimation', *Technometrics*, Vol. 12, No. 3, pp.591–612.

Migdadi, Y. and Omary, O. (2017) 'The impact of banks adoption of multi-channels mix on the internet banking service encounter quality: the case of Arab middle east region', *International Journal of Services and Standards*, Vol. 12, No. 1, pp.47–63, https://doi.org/10.1504/ijss.2017.10009316

Moffitt, K.C. and Vasarhelyi, M.A. (2013) 'AIS in an age of big data', *Journal of Information Systems*, Vol. 27, No. 2, pp.1–19.

Mohamed, I.S. and Marthandan, G. (2019) 'Determinants of e-business usage in Malaysian service industry', *International Journal of Services and Standards*, Vol. 13, Nos. 1–2, pp.59–82.

Nash, K.S. (2019) 'Cyber daily: angry shareholders to seek proof of prudent cyber tactics', *The Wall Street Journal*, 29 January, https://www.wsj.com/articles/cyber-daily-angry-shareholders-to-seek-proof-of-prudent-cyber-tactics-11548764969

Natter, A. (2021) *US Pipeline Watchdog Rebuffed Call for Cybersecurity Rules*, Bloomberg. com, 12 May, https://www.bloomberg.com/news/articles/2021-05-12/u-s-pipeline-watchdog-has-6-staff-no-cybersecurity-regulations

Rahman, A.R. and Debreceny, R.S. (2014) 'Institutionalized online access to corporate information and cost of equity capital: a cross-country analysis', *Journal of Information Systems*, Vol. 28, No. 1, pp.43–74.

Renaud, K., Orgeron, C., Warkentin, M. and French, P.E. (2020) 'Cyber security responsibilization: an evaluation of the intervention approaches adopted by the five eyes countries and China', *Public Administration Review*, Vol. 80, No. 4, pp.577–589.

Reuters (2021) *Colonial Pipeline Hackers Stole Data on Thursday – Bloomberg News*, 9 May, https://www.reuters.com/business/energy/colonial-pipeline-hackers-stole-data-thursday-bloomberg-news-2021-05-09/

Rosati, P., Gogolin, F. and Lynn, T. (2020) 'Cyber-security incidents and audit quality', *European Accounting Review*, pp.1–28.

Satariano, A. (2019) 'Google is fined $57 million under Europe's data privacy law', *The New York Times*, 21 January, Retrieved 14 February, 2021, from https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html

Securities and Exchange Commission (SEC) (2021) *SEC Announces Three Actions Charging Deficient Cybersecurity Procedures*, 30 August, Retrieved 1 October 2021, from https://www.sec.gov/news/press-release/2021-169

Smith, T.J. (Tom), Higgs, J.L. and Pinsker, R.E. (2019) 'Do auditors price breach risk in their audit fees?', *Journal of Information Systems*, Vol. 33, No. 2, pp.177–204.

Spamann, H. (2009) 'The 'anti-director rights index' revisited', *Review of Financial Studies*, Vol. 23, No. 2, pp.467–486.

Srinivasan, S., Wahid, A.S. and Yu, G. (2015) 'Admitting mistakes: home country effect on the reliability of restatement reporting', *The Accounting Review*, Vol. 90, No. 3, pp.1201–1240.

Sutton, P. (2019) *Important Lessons from Germany's First GDPR-Related Fine*, 16 January 2019, Retrieved 14 February, 2021 from https://www.radiusworldwide.com/blog/2019/1/important-lessons-germany-s-first-gdpr-related-fine

Taylor, C. (2021) *WhatsApp Says European Users Do not Have to Share Data with Facebook*, 7 January, Retrieved 14 February, 2021, from https://www.irishtimes.com/business/technology/whatsapp-says-european-users-do-not-have-to-share-data-with-facebook-1.4452435

Telang, R. and Wattal, S. (2007) 'An empirical analysis of the impact of software vulnerability announcements on firm stock price', *IEEE Transactions on Software Engineering*, Vol. 33, No. 8, pp.544–557.

Wang, C. (2019) *Corporate Boards are Snatching Up Cybersecurity Talents*, Forbes, 30 August, https://www.forbes.com/sites/chenxiwang/2019/08/30/corporate-boards-are-snatching-up-cybersecurity-talents/?sh=679dd31e479f

Wen, H., Koong, K.S. and Liu, L.C. (2015) 'Some observations on the US e-commerce trade statistics', *International Journal of Services and Standards*, Vol. 10, No. 3, pp.148–168.

Yen, J-C., Lim, J-H., Wang, T. and Hsu, C. (2018) 'The impact of audit firms' characteristics on audit fees following information security breaches', *Journal of Accounting and Public Policy*, Vol. 37, No. 6, pp.489–507.

Zagorchev, A.G., Vasconcellos, G. and Bae, Y. (2011) 'The long-run relation among financial development, technology and GDP: a panel cointegration study', *Applied Financial Economics*, Vol. 21, No. 14, pp.1021–1034.

Zhuang, Y., Choi, Y., He, S., Leung, A.C.M., Lee, G.M. and Whinston, A. (2020) 'Understanding security vulnerability awareness, firm incentives, and ICT development in pan-Asia', *Journal of Management Information Systems*, Vol. 37, No. 3, pp.668–693.

Zukis, B. (2020) *Cybersecurity Regulation and Litigation: The* 800 *Pound Gorilla in the Boardroom*, Retrieved 14 February 2021, from https://www.forbes.com/sites/bobzukis/2020/12/01/cybersecurity-regulation-and-litigation-the-800-pound-gorilla-in-the-boardroom/?sh=3165fc6032ef