Journal of Operational Risk **15**(4), 1–24
DOI: 10.21314/JOP.2020.249

Risk journals

Research Paper

The spillover effect of the Bangladesh Bank cyber heist on banks' cyber risk disclosures in Bangladesh

Mohammed Mehadi Masud Mazumder and Md Abdus Sobhan

[1]Department of Accounting and Financial Management, Newcastle Business School, Northumbria University, Newcastle upon Tyne NE1 8ST, UK;
emails: mohammed.mazumder@northumbria.ac.uk, abdus.sobhan@northumbria.ac.uk

(Received April 4, 2020; revised September 29, 2020; accepted October 19, 2020)

ABSTRACT

Bangladesh Bank (BB), the central bank of Bangladesh, experienced a highly organized cyber heist in February 2016 that seriously impaired the legitimacy of the cyber security systems of the country's overall banking sector. This study examines the spillover effect of that cyber heist on the cyber risk disclosures of the banking sector in Bangladesh. Building on institutional theory, we propose that in emerging markets, after a notable cyber heist experienced by the country's central bank, the banking sector of the country tends to increase cyber risk disclosures as an institutional strategy to regain legitimacy. Analyzing the disclosures in the annual reports of 38 commercial banks from 2014 to 2018, we find that banks' cyber risk disclosures significantly increased after the BB cyber heist. We also find that the political embeddedness of the banks and their adherence to Islamic Shariah negatively influence a bank's tendency to use cyber risk disclosures as a legitimacy-regaining strategy after the heist. Our institutional perspective offers new insights into why the banks in an emerging country engage more in cyber risk disclosures after such an atrocious cyber attack.

Corresponding author: M. A. Sobhan

Print ISSN 1744-6740 | Online ISSN 1755-2710

Keywords: cyber risk disclosures; Bangladesh Bank (BB) heist; institutional theory; politically embedded banks; Islamic Shariah-based banks; Bangladesh.

1 INTRODUCTION

Banks have attracted significant cyber security threats in recent years because they deal with money and "money has become a particularly important motivation for malicious and criminal hackers over the last two decades" (Holt and Kilger 2012, p. 10). Cyber security breaches may negatively affect the focal firm's market value (Richardson *et al* 2019; Lange and Burger 2017) and competitive advantage while increasing its operational costs, such as additional investment in cyber security protection and remediation payments (Bodin *et al* 2018; Securities and Exchange Commission 2011). Amid this growing concern about cyber risks, stakeholders want to understand how banks are guarding against and responding to cyber threats. To alleviate stakeholders' concerns and to reassure them, banks could disclose more information on the cyber risks they face as well as their strategies to manage those risks. Cyber risk disclosures may help banks demonstrate their commitment toward cyber security for external stakeholders, better understand which cyber security measures are crucial to combat cyber threats, and increase cyber risk awareness of internal and external stakeholders (Berkman *et al* 2018).

Despite the importance and benefits of cyber risk disclosures, prior studies mainly examine their economic impact (see, for example, Berkman *et al* 2018; Morse *et al* 2017; Gordon *et al* 2010) in response to the recent guidelines (see, for example, Financial Reporting Council 2016; Securities and Exchange Commission 2011) and reporting framework (see, for example, Institute of Chartered Accountants of England and Wales 2018; American Institute of Certified Public Accountants 2017) on cyber risk disclosures in developed countries. Limited research also investigates the impact of a cyber security breach on the shareholder wealth of the focal firms (see, for example, Richardson *et al* 2019; Lange and Burger 2017) or intra-industry members (see, for example, Kashmiri *et al* 2017). In contrast, there is a lack of studies examining the effect of a cyber incident on cyber risk disclosures by a focal firm, let alone the spillover effect on cyber risk disclosures by firms that have not experienced a cyber security breach themselves. Further, most of the prior studies on the consequence of cyber security breaches focus on developed countries, mainly the United States. One reason for this could be that the regulatory agencies and accounting professions in many developing countries have yet to offer any guidance or framework on cyber risk disclosures. A study on the spillover effect of a cyber security incident on cyber risk disclosures in the context of a developing country is therefore warranted.

As such, we investigate the level of cyber risk disclosures by the banking sector in Bangladesh, an emerging economy, after the Bangladesh Bank (BB) cyber heist. The BB heist, a highly organized cyber heist that sent shock waves around the world and revealed the cracks and vulnerabilities in the international banking community (Hofileña and Sy 2017), was exposed in February 2016. Based on media reports and related literature, we argue that, as BB is the regulator of the country's banking sector and the heist could have been the biggest bank heist in history (Hofileña and Sy 2017), the BB heist severely impaired the legitimacy of the banking sector of Bangladesh. Drawing on insights from institutional theory (Scott 2014; DiMaggio and Powell 1983; Meyer and Rowan 1977) and extant prior research on voluntary disclosures which perceives disclosures as one of the crucial institutional strategies to repair and regain damaged legitimacy (see, for example, Marquis and Qian 2014; Lim and Tsutsui 2012; Campbell 2007; Bansal 2005), we hypothesize that the banking sector of Bangladesh will disclose more information on cyber risks to regain their impaired legitimacy (Suchman 1995) after the BB heist.

We then build on organizations' diverse strategic responses to institutional demands (Pache and Santos 2010; Oliver 1991) and propose that the political embeddedness and Islamic orientation of banks will influence their perception of legitimacy gain through increased cyber risk disclosures after the BB heist. These banks differ from their counterparts in terms of dependence on, and power of, divergent institutional constituents that affect norms, expectations and responsibilities. Hence, the political embeddedness and Islamic orientation of banks will affect the extent of increased cyber risk disclosures after the BB heist.

We conduct a content analysis of 38 banks' annual reports to specifically investigate the changes in banks' cyber risk disclosures from 2014 to 2018. We find evidence that, in general, there is a significant increase in cyber risk disclosures by banks after the BB heist. When analyzed through the lens of sociological institutional theory, our findings suggest that banks indeed engaged in legitimacy-regaining strategies by increasing cyber risk disclosures after the legitimacy of the sector was threatened by the cyber heist experienced by their regulatory agency, BB. We also find that the increase in cyber risk disclosures was lower for both politically embedded and Islamic Shariah-based banks. Our findings suggest that politically embedded banks achieving greater political legitimacy have fewer incentives to gain legitimacy from the public by making increased cyber risk disclosures after the BB heist. Similarly, Islamic banks may perceive a smaller gain in legitimacy from increased cyber risk disclosures, possibly because of better congruence between Islamic banks' compliance with the Shariah and Islamic religious beliefs of most of their customers, which offers some inherent legitimacy.

In Section 2, we present an overview of the banking sector of Bangladesh. In Section 3, we discuss the BB heist and the resultant loss of legitimacy by cyber security

systems in Bangladesh's banking sector. In Section 4, we analyze our theoretical viewpoint and develop our hypotheses. The methodology of the study is described in Section 5. Section 6 presents the findings of this study. In Section 7, we offer some discussion and state the conclusions, implications and limitations of this study.

2 A BRIEF OVERVIEW OF THE BANGLADESH BANKING SECTOR

Bangladesh became independent from Pakistan in 1971. After independence, the new government embarked on socialism (Ahamed 1978). The government merged and grouped all the banks operating in Bangladesh into six commercial banks and nationalized them (Bangladesh Bank 2018). Within a few years, state-owned enterprises became inefficient and accumulated enormous operating losses due to the politicization and corruption of the management (Ghafur 1976; Ahmad 1976). As a result, Bangladesh adopted market-based capitalism in 1975 (Sobhan 2016). The subsequent government privatized three of the six state-owned banks in 1985 and also provided licences for private entrepreneurs to operate banking business (Nuruzzaman 2004). Of the banks floated under the private initiatives, several were established according to (or later converted to) Islamic Shariah principles, possibly to capitalize on the religious ideology of most of the population of Bangladesh. The government also founded a few specialized banks under state ownership to promote the economic development of specific sectors such as agriculture and small and medium-sized industries. At present, Bangladesh has 56 scheduled commercial banks consisting of 6 state-owned banks, 2 specialized banks, 9 foreign banks and 39 private commercial banks, of which 7 are Islamic Shariah-based banks (Bangladesh Bank 2016), although BB, as the central bank of the country, is responsible for prescribing policies to emphasize risk management and for monitoring the implementation of those policies by non-state-owned banks, which are supervised and controlled by the bank and financial institution division of the Ministry of Finance (Byron and Chakma 2019).

3 THE CYBER HEIST AND THE LOSS OF LEGITIMACY OF THE CYBER SECURITY SYSTEMS IN BANGLADESH'S BANKING SECTOR

BB, the central bank of Bangladesh, like the other 250 central banks and governments of the world, maintains its foreign reserve account at the Federal Reserve Bank of New York (Hammer 2018). Unfortunately, in February 2016, BB became the victim of the first and most severe cyber theft from a central bank using the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system. The cyber criminals attempted to steal nearly US$1 billion from BB's foreign reserve

account by sending 35 apparently legitimate payment orders to the Federal Reserve Bank (Hammer 2018).

A payment involving US$20 million to an account in the name of the Shalika Foundation in Sri Lanka was blocked by Deutsche Bank, the intermediary bank between Pan Asia Bank and the Federal Reserve Bank, when a banker at Pan Asia Bank questioned such a large payment to a small NGO and the Deutsche Bank also noticed the misspelling of "Foundation" as "Fandation" (Hammer 2018). This US$20 million was later recovered by BB. Four transactions had been carried out successfully by transferring US$81 million to four suspicious accounts at Rizal Commercial Banking Corporation in the Philippines and had then been remitted to the casino industry via an account in the name of William So Go and Philrem, a remittance company. The remaining 30 mysterious orders (worth US$850 million) were not carried out, thanks to the similarity between the names of the Rizal Commercial Banking Corporation branch "Jupiter" and Jupiter Seaways Shipping, an Athens-based firm that was blacklisted for evading sanctions against Iran (Hammer 2018).

The event became public in March 2016 and sent shock waves around the world, revealing the cracks and vulnerabilities in the international banking community (Hofileña and Sy 2017). In Bangladesh, the exposure of the heist created serious discontent among the public and disappointment for BB. Critics questioned the strength of cyber security of BB. In the parliament and the media, the government was also accused of failing to protect the hard-earned foreign currency of the country.

The government and BB took many immediate actions to appease the public outcry and tried to repair their impaired legitimacy. These actions included

- the immediate dismissal of Atiar Rahman, the governor of BB at the time of the cyber heist, and two of his deputy governors from their positions;
- the commissioning of a probe committee chaired by Dr Mohammed Farashuddin, a former governor of BB, which included a computer science professor from Bangladesh University of Engineering and Technology and an additional secretary at the Ministry of Finance;
- the launching of an investigation by the Criminal Investigation Department that was later joined by the US Federal Bureau of Investigation; and
- the appointment of at least two groups of external information technology experts, including Mandiant, a unit of the FireEye cyber security group, and World Informatix, an Indian IT firm, to probe the theft and make recommendations for strengthening the cyber security of the BB's network systems (Hammer 2018; Byron 2016).

Although publication of the full report by the probe committee was banned by the government, possibly because of the fear of further loss of legitimacy, the head of the probe committee reported to the media that the heist was the outcome of irresponsible behavior by a few officials at BB, the SWIFT system and the Federal Reserve Bank (*Daily Star* 2016). This claim is consistent with those of others who investigated the heist (see, for example, Hammer 2018; Shibli 2016). For instance, Hammer (2018) maintained that the hackers were successful in introducing malware into BB's computer system not only to take control of the system but also to manipulate the SWIFT software. The head of the probe committee also reported that the cyber theft caused a lot of damage to the BB and acted as a warning to the country's banking sector (Byron and Rahman 2016). In summary, in addition to highlighting the vulnerability of the SWIFT system, which was perceived to be impenetrable (Hammer 2018), the heist threatened the legitimacy of the cyber security system of the BB as well as of the Bangladesh banking sector. It also exposed the banking sector in Bangladesh to an increasing number of cyber threats, as hackers would easily perceive the vulnerability of the cyber security in this sector.

4 THEORETICAL FRAMEWORK AND DEVELOPMENT OF HYPOTHESES

4.1 Institutional theory and accounting disclosure as an institutional strategy to regain legitimacy

Legitimacy, political economy and institutional theories have all been used in the past to enhance our understanding of voluntary, nonfinancial accounting disclosure (see, for example, Blanc *et al* 2019; Marquis and Qian 2014; Lim and Tsutsui 2012; Belal and Cooper 2011; Cho 2009; Campbell 2007; Bansal 2005). Legitimacy theory maintains that a "social contract" exists between a firm and society at large and therefore it best explains the overall increases in voluntary accounting disclosures after environmental incidents that question legitimacy (see, for example, Cho 2009; Deegan *et al* 2000). Similarly, political economy theory is mainly employed to explain cross-country divergence in voluntary accounting disclosures (see, for example, Lim and Tsutsui 2012) and nondisclosure of voluntary accounting information, as silence better serves the interest of powerful managers (see, for example, Belal and Cooper 2011). In contrast, institutional theory is used to explain both the overall increases and the variation in voluntary disclosures among firms because of their relative dependence on particular institutional constituents (see, for example, Marquis and Qian 2014; Campbell 2007; Bansal 2005). Hence, we believe that institutional theory is the more pertinent theoretical framework for this study, as we intend to study both purposes.

Institutional theory proposes that organizations' actions are influenced by social pressure (Scott 2014; DiMaggio and Powell 1983; Meyer and Rowan 1977), as organizations require approval from institutional constituents to secure resources and ensure survival (Scott 2014; Deephouse 1999). To get this approval from institutional constituents, organizations need to gain and maintain legitimacy, which refers to "a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions" (Suchman 1995, p. 574). Legitimacy concerns, therefore, motivate the organizations to adopt socially desirable practices (Deephouse 1999).

However, recent theoretical development suggests that organizations that face diverse demands from different institutional constitutes purposefully and strategically select their responses to institutional pressures as active agents (Pache and Santos 2010; Oliver 1991). This perspective maintains that organizations' responses to institutional demands are influenced by, for example, perceived legitimacy gain from the implementation of the recommended practices (Scott 2014, p. 73), the organization's relative dependence on and power over institutional constituents (Oliver 1991), the consistency between organizational-level dynamics and institutional demands (Shipilov *et al* 2010). As such, organizations' strategic responses to institutional pressures are diverse rather than uniform (Rao *et al* 2000).

4.2 Development of our hypotheses

4.2.1 Cyber risk disclosures as a legitimacy-regaining strategy after the BB heist

The BB heist was widely publicized in both the local and international media because it was the first cyber heist experienced by a country's central bank (Hofileña and Sy 2017), and it is believed to have been the largest successful cyber theft at a financial institution at that time (US Justice Department 2018). Many of these media reports questioned the legitimacy of the cyber security systems of not only BB but also the banking sector of the country (see, for example, Hammer 2018; Shibli 2016). For instance, the chairman of the probe committee formed by the government mentioned that the BB heist acted as a warning to the banking sector of Bangladesh to strengthen cyber security (Byron and Rahman 2016). In summary, the media reports and the above cautioning by the chairman of the probe committee brought disgrace to the cyber security systems of the Bangladesh banking sector. Under such circumstances, it is to be expected that the public, which is the most important institutional constituent for banks, will question the legitimacy of the cyber security systems of the Bangladesh banking sector and thus banks' ability to protect their customers' deposits and personal information from cyber criminals. This inability of banks,

in turn, may result in uncertainty over their future survival and the success of the banking sector of Bangladesh (see Ruef and Scott 1998).

Pioneer institutional theorists (see, for example, Meyer and Rowan 1977) maintain that firms experiencing a loss of legitimacy would adopt a variety of highly visible and relevant strategies to regain legitimacy from their institutional constituents. In the case of firms exposed to a cyber heist, cyber risk disclosures can be such a legitimacy-regaining strategy. There are many reasons for the success of this strategy. Cyber risk disclosures offer an opportunity to demonstrate a bank's commitment toward its cyber security protection efforts (Berkman *et al* 2018). They also aid our understanding of which cyber security measures are effective in combatting cyber security risks, which cyber security risks have emerged recently and need the most attention, and how to improve the cyber security risk awareness of internal and external stakeholders (Berkman *et al* 2018). A significant body of literature on corporate voluntary disclosure provides empirical support that companies increase voluntary disclosures after experiencing a legitimacy-threatening event (see, for example, Blanc *et al* 2019; Cho 2009; Deegan *et al* 2000). Therefore, it is reasonable to hypothesize that the banking sector of Bangladesh would likely have increased their level of voluntary disclosures concerning their cyber risk management activities after the BB heist. Of course, the question as to whether or not the banks in Bangladesh did increase their cyber risk disclosures after the BB heist is an empirical issue that can be tested. In terms of an alternative hypothesis, this could be stated as follows.

(H1A) The BB cyber heist resulted in a significant increase in the voluntary disclosure of cyber risks in banks' annual reports.

4.2.2 Political embeddedness of banks and the extent of increased disclosure on cyber risks after the BB heist

The politically embedded firms have multiple ties with the government (Okhmatovskiy 2010). These ties include dominant state ownership (Marquis and Qian 2014; Okhmatovskiy 2010), the national political appointment of the board of directors and executives (Marquis and Qian 2014), and the resultant close relationship between the government and firm executives (Zhang *et al* 2020), as well as significant influence by the government on the strategic and operational decisions of firms (Zhang *et al* 2020). Because of these ties, these firms enjoy preferential access to valuable resources controlled by the government (Faccio 2006; Wang *et al* 2008) or even obtain "protection" (Li and Zhang 2007, p. 794) when they are in distress. On the other hand, the government tends to pursue its political or socioeconomic goals using the resources of these firms (Okhmatovskiy 2010). While the multiple ties with the government facilitate the "political legitimacy" of politically embedded firms, they

weaken the motivation of politically embedded firms to use activities such as voluntary accounting disclosures to seek legitimacy from other institutional constituents (Marquis and Qian 2014). Consistent with this argument, several prior empirical studies show that political embeddedness adversely affects the quantity of voluntary disclosures (see, for example, Muttakin *et al* 2018; Marquis and Qian 2014; Chaney *et al* 2011).

In Bangladesh, the government owns a substantial percentage of shares in state-owned commercial banks (Sobhan and Bose 2019). It also controls these banks by appointing a highly politicized board of directors (Rahman and Khan 2012) and management, and injects resources when required (Byron and Chakma 2019). These banks not only implement the government agenda by disbursing loans to government-prioritized sectors but also offer loans at a preferential rate of interest, without adequate collateral, to business owners who are politically affiliated (Rahman and Khan 2012). In return, when these banks fall into financial distress because of a significant percentage of nonperforming loans, the government uses taxpayers' money to rescue them (Byron and Chakma 2019). Therefore, the principal institutional constituent for politically embedded banks is the government of Bangladesh rather than the public, as the survival and success of state-owned banks in Bangladesh are dependent on the legitimacy granted by the government. Moreover, the board of directors and executive management of these banks, because of their close relationship with the relatively unaccountable powerful government, have less motivation to remain accountable to the public. Consequently, politically embedded banks may have less incentive to regain public trust in their cyber security systems and therefore may have had less motivation to make increased cyber risk disclosures than private commercial banks after the BB heist. We therefore hypothesize the following.

(H2A) The BB heist resulted in a smaller increase in the voluntary disclosure of cyber risks by politically embedded banks than by private commercial banks in their annual reports.

4.2.3 Islamic Shariah-based banks and the extent of increased disclosure on cyber risks after the BB heist

The moral view of sociological institutional theory suggests that legitimacy gains from extended cyber risk disclosures are probably higher for Islamic banking than for conventional banking (Haniffa and Hudaib 2007). Societal demands for transparency and better protection of stakeholders' interests are greater for Islamic banking because these banks adhere to the Shariah principle (Elamer *et al* 2017). The Shariah principle suggests strict compliance with ethics, social responsibilities and protection of stakeholders' interests. Moreover, organizational-level dynamics of Islamic banking, such as Shariah-based operational guidelines and culture, are more

consistent with stricter internal control and better transparency (Belal *et al* 2019). Consistent with this view, extant research provides empirical evidence that Islamic banking makes more extensive disclosures on general risks (see, for example, Al-Bassam *et al* 2017; Elamer *et al* 2017) as well as operational risks (see, for example, Hermit 2019). In Bangladesh, prior research evidenced that Islamic banks disclose significantly more information on financial inclusion (Bose *et al* 2016) and sustainability (Sobhani *et al* 2012) than conventional banks.

In contrast, Islamic tag allows Islamic banks to earn too much customer allegiance intrinsically over their counterparts. Customers of Islamic banks are so loyal that being Islamic in operation dominates other values and bank performance indicators, including cyber risk management. Such inherent legitimacy may allow Islamic banks to become less sincere than conventional banks in regaining any legitimacy lost due to the BB cyber heist through cyber risk disclosures. Nobanee and Ellili (2016) argue that Islamic banks face less disclosure pressure than conventional banks because they conform to Islamic principles and ethics. They also argue that Islamic banks confronting lower financial constraints and market competition than conventional banks are less responsive to the external pressure and demands of stakeholders and hence are more reluctant to showcase their actions through disclosures.[1] Nobanee and Ellili also find support in favor of the arguments mentioned above.

Based on the above competing theoretical justifications and supporting empirical evidence, the influence of a bank's Islamic orientation on cyber risk disclosures is ex ante unclear. We therefore explore the effect of a bank's Islamic orientation on cyber risk disclosures by testing the following hypothesis.

(H3A) The increase in voluntary disclosure on cyber risks in annual reports as a result of the BB heist will be influenced by the Islamic orientation of banks.

5 RESEARCH METHODS

5.1 Sample selection

On the eve of the BB heist, Bangladesh had 56 scheduled commercial banks, consisting of 6 state-owned commercial banks (denoted as "politically embedded"[2] commercial banks in this study), 2 specialized banks, 9 foreign banks and 39 private commercial banks, including 7 Islamic Shariah-based banks. All the scheduled commercial banks (private as well as state-owned), of which 30 are listed on the Dhaka Stock Exchange (the oldest and the biggest stock exchange in Bangladesh), were selected for analysis. We intentionally excluded nine foreign banks, as they may

[1] Conventional commercial banks do not explicitly claim to operate following Islamic Shariah.
[2] See Section 4.2.2 for details.

have heterogeneous disclosure behavior, unlike local banks, due to significant foreign ownership and globalized operation. We also did not consider banks established for specialized purposes (for example, Bangladesh Krishi Bank and Rajshahi Krishi Unnayan Bank), as they do not provide the same range of services as scheduled commercial banks. The annual reports (from 2014 to 2018) available for each of the banks were collected from their websites. The sample selection process eventually ended up with 38 commercial banks (3 state-owned (politically embedded) commercial banks and 35 private commercial banks) resulting in 190 bank–year observations for the sample period (2014–18).[3] Also, in terms of Islamic and conventional classification, out of 38 sample banks, 6 commercial banks followed Islamic Shariah operation.

5.2 Data collection

Like previous studies on risk reporting (see, for example, Mazumder and Hossain 2019; Li *et al* 2018; Allini *et al* 2016; Elshandidy and Shrives 2016; Elshandidy *et al* 2013; Abraham and Cox 2007), we have adopted content analysis to measure the extent of cyber-related risk disclosures in a complete annual report. As an automated method of content analysis is considered to be more accurate and has an edge over the manual method (Li *et al* 2018; Saggar and Singh 2017; Allini *et al* 2016; Elshandidy and Neri 2015; Elshandidy *et al* 2013), we ran a text search query using NVIVO 12 software to identify the cyber risk disclosures in the annual reports. Following prior disclosure studies (see, for example, Li *et al* 2018; Saggar and Singh 2017; Nelson and Pritchard 2016; Campbell *et al* 2014; Li 2010; Abraham and Cox 2007), we counted one keyword as a unit of analysis. Though previous risk disclosure studies have also adopted content analysis with one sentence as a unit of analysis (see, for example, Oliveira *et al* 2011; Amran *et al* 2009; Linsley and Shrives 2006), several researchers (see, for example, Saggar and Singh 2017; Milne and Adler 1999) are critical of counting sentences as this involves a few constraints that limit the effectiveness of sentence-level analysis in the empirical studies. More specifically, using the sentence as a unit of measurement may overlook the possibility that differences in the use of grammar might result in two different writers conveying the same message in a different number of sentences (Unerman 2000). Moreover, counting sentences is more subjective than relying on relevant keywords, as risk information is diluted into the mass of other information usually provided in the annual report (Beretta and Bozzolan 2004) and it would be difficult for readers to locate the same information (Saggar and Singh 2017). Milne and Adler (1999) argued that words add

[3] Seven banks were excluded due to unavailability of the annual reports on their websites for the sample period. The average size of the sample banks measured by total assets is Tk2 66 978 million (approximately US$3150 million).

more precision to measurement. Based on prior research on cyber risk disclosures (Li *et al* 2018; Wang *et al* 2013; Gordon *et al* 2010), 54 keywords related to cyber risk disclosures were identified and refined to prevent misidentification.[4] To ensure the quality of identification, we randomly selected 20 annual reports and manually validated the disclosures related to cyber risks. All of them were accurately identified. (Appendix A online provides a list of these keywords.)

5.3 Data analysis

To test hypothesis H1A, we compared the means (medians) of the cyber risk disclosures before and after the BB heist using a t-test (a Wilcoxon rank sum test). Hypothesis H2A was also tested by comparing the means (medians) of the cyber risk disclosures of private commercial banks and politically embedded banks both before and after the BB heist. Similarly, we tested hypothesis H3A by comparing the means (medians) of cyber risk disclosures of conventional commercial banks and Islamic Shariah-based banks both before and after the BB heist.

6 FINDINGS

6.1 Overall trend of cyber risk disclosures

Figure 1 depicts year-wise longitudinal patterns of total cyber risk disclosures by the sample banks. It is evident that total cyber risk disclosures increased over the study period (2014–18). While the total cyber risk disclosures increased by approximately 38% from 2014 to 2015, they increased by 60% from 2015 to 2016, which was basically the year when BB encountered the notorious cyber heist. This evidence provides preliminary support for our hypothesis H1A, ie, that the level of cyber risk disclosures in the annual reports increased significantly after the BB heist in 2016.

To provide more definite empirical evidence in support of hypothesis H1A, we compared the means and medians of cyber risk disclosures before (2014 and 2015) and after (2016–18) the BB heist using a two-sample t-test and Wilcoxon rank sum test, respectively. The results are reported in Table 1, which shows that the mean (median) of cyber risk disclosures after the BB heist is significantly greater than the mean (median) of cyber risk disclosures before the BB heist at the 1% level. These results thus support hypothesis H1A, indicating that, on average, the banking sector of Bangladesh voluntarily disclosed more information on cyber risks to regain their legitimacy, which was sternly tarnished by the BB cyber scandal in February 2016.[5]

[4] All the words/phrases are stemmed.

[5] As the cyber risk disclosures level shows an increasing trend since 2014, we also conducted a year-wise t-test (ie, between 2014 and 2015, 2015 and 2016, and so on) comparing the mean cyber risk disclosures. Except for the mean difference between 2015 and 2016 (t-value $= 2.61$,

FIGURE 1 Cyber risk disclosures by year from 2014 to 2018.

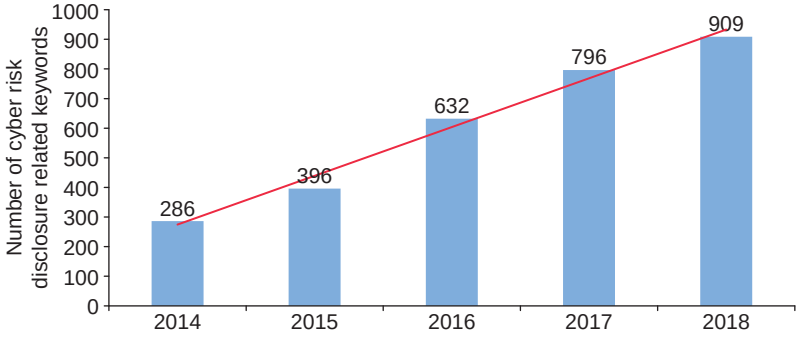


TABLE 1 Univariate test comparing cyber risk disclosures before (2014–15) and after (2016–18) the BB heist.

	Before scandal	After scandal	t/z-value	p-value
Mean	8.97	20.50	6.477	0.0000*
Median	7.00	18.00	6.354	0.0000*

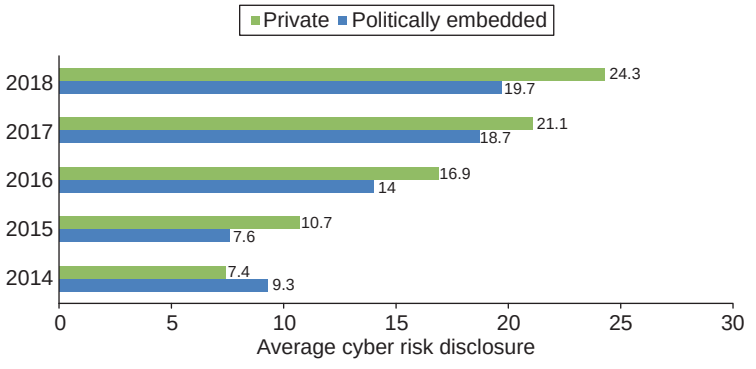
Number of observations: 76 before scandal, 114 after scandal. Difference in means is tested using t-test with unequal variance. Difference in medians is tested using Wilcoxon rank sum (Mann–Whitney) test. *Significance at the 1% level (one-tail).

6.2 Cyber risk disclosures between private and politically embedded commercial banks compared

Figure 2 presents the year-wise average cyber risk disclosures for private commercial banks and politically embedded commercial banks from 2014 to 2018. Throughout the study period, on average, private commercial banks dominate politically embedded commercial banks in terms of cyber risk disclosures in every period except 2014. Moreover, the trend of growth in the average cyber risk disclosures of private commercial banks is more exponential than that of politically embedded commercial banks. These findings are consistent with our hypothesis H2A, ie, unlike private commercial banks, politically embedded banks have less motivation to increase

$p = 0.006$), none of the other yearly mean differences are statistically significant at a 5% level. This evidence adds further support to our hypothesis H1A, given that BB experienced the cyber heist in February 2016. For brevity, we do not report the detailed year-wise results.

FIGURE 2 Year-wise average cyber risk disclosures (2014–18) for private commercial banks and politically embedded commercial banks.



cyber risk disclosures as a legitimacy-regaining strategy after the BB heist, as they are more reliant on the government than on the general public for legitimacy.

To offer further statistical evidence for hypothesis H2A, we compared the means and medians of cyber risk disclosures of private commercial banks and politically embedded commercial banks for two periods: before the BB cyber heist (2014–15), and after the BB cyber heist (2016–18). The results are reported in parts (a) and (b) of Table 2, respectively.

Table 2(a) shows that before the BB heist the mean (median) of cyber risk disclosures of private commercial banks is not statistically different from the mean (median) of politically embedded commercial banks at a conventional significance level. However, after the BB heist, the mean of cyber risk disclosures as reported in the annual reports of private commercial banks is higher than the mean of cyber risk disclosures as reported in annual reports of politically embedded commercial banks at the 10% significance level (see Table 2(b)). This result supports our hypothesis H2A, ie, the politically embedded banks' high dependence on government for legitimacy makes them a bit reluctant to use cyber risk disclosures as a legitimacy-seeking strategy after the BB heist. Our finding is consistent with past empirical evidence that political embeddedness negatively influences the quantity of voluntary disclosure (see, for example, Muttakin *et al* 2018; Marquis and Qian 2014; Chaney *et al* 2011).

TABLE 2 Univariate test comparing cyber risk disclosures between private commercial banks and politically embedded commercial banks before and after the BB heist.

(a) Before the heist

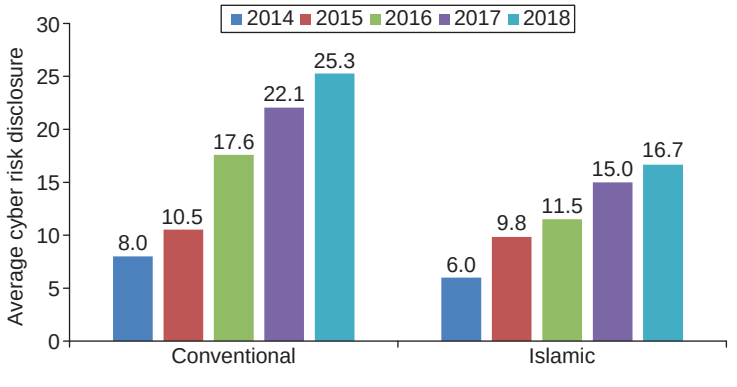
	Private commercial banks	Politically embedded banks	t/z-value	p-value
Mean	9.014	8.50	0.145	0.4447
Median	7.00	7.50	0.097	0.9229

(b) After the heist

	Private commercial banks	Politically embedded banks	t/z-value	p-value
Mean	20.762	17.444	1.400	0.0862**
Median	18.00	20.00	0.084	0.9330

There were 70 observations for private commercial banks and 6 observations for politically embedded banks before the heist and 105 observations for private commercial banks and 9 observations for politically embedded banks after the heist. The difference in means is tested using the t-test with unequal variance. The difference in medians is tested using the Wilcoxon rank sum (Mann–Whitney) test. **Significance at the 10% level (one-tail).

FIGURE 3 Comparison of year-wise average cyber risk disclosures between conventional and Islamic Shariah-based commercial banks.



6.3 Cyber risk disclosures between conventional and Islamic Shariah-based commercial banks compared

Figure 3 depicts the average cyber risk disclosures of conventional commercial banks and Islamic Shariah-based commercial banks over the sample period. It

TABLE 3 Univariate test comparing cyber risk disclosures between conventional commercial banks and Islamic Shariah-based commercial banks before and after the BB heist.

(a) Before the heist

	Conventional banks	Islamic Shariah-based banks	t/z-value	p-value
Mean	9.266	7.417	0.701	0.2465
Median	8.00	5.00	0.780	0.4353

(b) After the heist

	Conventional banks	Islamic Shariah-based banks	t/z-value	p-value
Mean	21.646	14.389	2.679	0.0052*
Median	19.50	12.00	1.730	0.0836**

There were 64 observations for conventional banks and 12 observations for Shariah-based banks before the heist and 96 observations for conventional banks and 18 observations for Shariah-based banks after the heist. The difference in means is tested using a t-test with unequal variance. The difference in medians is tested using a Wilcoxon rank sum (Mann–Whitney) test. * and ** indicate significance at the 1% level (one-tail) and the 10% level (one-tail), respectively.

clearly shows that conventional banks provide more cyber risk disclosures, on average, compared with Islamic Shariah-based banks. Also, the year-wise increase in average cyber risk disclosures is much sharper for conventional banks than Islamic Shariah-based banks. This evidence contradicts our expectation (hypothesis H3A) and empirical evidence provided by the prior literature (see, for example, Al-Bassam *et al* 2017; Elamer *et al* 2017; Hermit 2019), ie, Islamic Shariah-based banks, because of their compliance with the Shariah principle, disclose more risk information.

Further statistical tests comparing the mean and median cyber risk disclosures of conventional banks with those of Islamic Shariah-based banks for the two periods before (2014–15) and after (2016–18) the BB heist support the descriptive findings presented above. We do not find any significant difference between the mean (median) cyber risk disclosures of conventional banks and Islamic Shariah-based banks before the BB heist (Table 3(a)).

However, we find that the mean (median) of cyber risk disclosures as reported in the annual reports of conventional banks is significantly higher at the 1% (10%)

level than the mean (median) of cyber risk disclosures as reported in annual reports of Islamic Shariah-based banks after the BB heist (Table 3(b)). These findings support our hypothesis H3A and may suggest that, after the BB heist, Islamic commercial banks, because of their compliance with the Islamic principles and ethics (Nobanee and Ellili 2016), received less legitimacy pressure for disclosures from the public than conventional banks. This may be more pronounced in Bangladesh because of the high level of congruence between Islamic Shariah-based banks' activities and the norms of acceptable behavior emanating from the religious belief of most of the population. Our evidence, although it contradicts prior evidence in Bangladesh (Bose *et al* 2016; Sobhani *et al* 2012), is consistent with Nobanee and Ellili (2016).

7 DISCUSSION AND CONCLUSION

This paper examined the spillover effect of the BB heist on the cyber risk disclosures of banks in Bangladesh. We discussed how the BB heist, the first cyber attack suffered by a central bank in history, created a threat to the legitimacy of the cyber security systems of the banks monitored by the BB. Following the institutional theory, we conceptualized cyber risk disclosures as a legitimacy-regaining strategy and developed three main hypotheses to evaluate the use of cyber risk disclosures by the banking sector of Bangladesh as well as by the politically embedded and Islamic Shariah-based banks as a legitimacy-regaining strategy after the BB heist. We find support for all three hypotheses.

As mentioned in Section 1, there is a lack of literature on the spillover effect of a cyber heist experienced by a regulatory agency on the cyber risk disclosures of regulated firms. The most relevant prior study is by Kashmiri *et al* (2017), who studied the contagion effect of the customer data breach at Tiger on the shareholder value of other US retailers. In contrast, our study focuses on the spillover effect of the atrocious cyber heist suffered by the central bank of an emerging economy on the cyber risk disclosures of the country's banking sector. By proving the positive spillover effect of a cyber heist experienced by a regulator on clients' cyber risk disclosures, this study adds to the emerging literature on the spillover effects of a major cyber heist.

Moreover, Gordon *et al* (2006) studied the effect of the Sarbanes–Oxley Act on information risk disclosures by US firms, but there is no such study in the context of emerging countries, possibly because cyber risk disclosure regulations and reporting frameworks have not yet been developed in the context of emerging countries. Using an appropriate theoretical framework, our study demonstrates that, despite this lack of cyber risk disclosure regulations and reporting frameworks, banks in emerging countries voluntarily increased cyber risk disclosures to regain the legitimacy impaired due to a major cyber heist. Further, our evidence on politically

embedded and Islamic Shariah-based banks' usage of cyber risk disclosures as a legitimacy-regaining strategy after the BB heist contradicts the prior literature on the legitimacy-seeking motives of politically embedded (Zhang *et al* 2020) and Islamic Shariah-based (Hermit 2020) banks. Our contradictory evidence may suggest that the legitimacy-seeking motives of politically embedded and Islamic Shariah-based banks are context dependent.

Finally, the findings of this study are also relevant to regulators and practitioners. Based upon the results, it appears that politically embedded and Islamic Shariah-based banks are reluctant to make cyber risk disclosures in annual reports. Hence, regulators and the accounting profession must develop cyber risk disclosure regulations and a reporting framework to ensure the consistency of cyber risk disclosures among different types of banks, so that the public can assess the cyber security systems of banks before engaging in banking activities.

The results of this study should be interpreted with caution, as voluntary cyber risk disclosures by banks may be limited in developing countries that do not experience critical cyber incidents. Hence, further studies are needed to understand the extent and dynamics of banks' cyber risk disclosures in other emerging economies. Future studies could use the disclosure-coding instrument that we developed (or a modified version of this instrument) to measure cyber risk disclosures. Moreover, we depend mainly on descriptive statistics and univariate statistical tests, and therefore our results on the impact of political embeddedness and Islamic Shariah compliance by banks could be affected by other bank-specific characteristics. Future studies could validate or refute our findings in Bangladesh by investigating the impact of political embeddedness and Islamic Shariah compliance on cyber risk disclosures by performing multivariate analysis.

DECLARATION OF INTEREST

The authors report no conflicts of interest. The authors alone are responsible for the content and writing of the paper.

ACKNOWLEDGEMENTS

We are grateful for the constructive and helpful comments of the editor-in-chief Marcelo Cruz, the guest editors of this special issue and three anonymous reviewers.

REFERENCES

Abraham, S., and Cox, P. (2007). Analysing the determinants of narrative risk information in UK FTSE 100 annual reports. *British Accounting Review* **39**(3), 227–248 (https://doi.org/10.1016/j.bar.2007.06.002).

Ahamed, E. (1978). Development strategy in Bangladesh: probable political consequences. *Asian Survey* **18**(11), 1168–1180 (https://doi.org/10.2307/2643299).

Ahmad, M. (1976). The historical perspective of public sector enterprises in Bangladesh. *Journal of Management Business and Economics* **2**(3), 252–294.

Al-Bassam, W. M., Ntim, C. G., Opong, K. K., and Downs, Y. (2018). Corporate boards and ownership structure as antecedents of corporate governance disclosure in Saudi Arabian publicly listed corporations. *Business and Society* **57**(2), 335–377 (https://doi.org/10.1177/0007650315610611).

Allini, A., Manes Rossi, F., and Hussainey, K. (2016). The board's role in risk disclosure: an exploratory study of Italian listed state-owned enterprises. *Public Money and Management* **36**(2), 113–120 (https://doi.org/10.1080/09540962.2016.1118935).

American Institute of Certified Public Accountants (2017). Reporting on an entity's cybersecurity risk management program and controls: attestation guide. Report, AICPA, New York.

Amran, A., Manaf Rosli Bin, A., and Che Haat Mohd Hassan, B. (2009). Risk reporting: an exploratory study on risk management disclosure in Malaysian annual reports. *Managerial Auditing Journal* **24**(1), 39–57 (https://doi.org/10.1108/02686900910919893).

Bangladesh Bank (2016). Annual report July 2015–June 2016. Bangladesh Bank, Dhaka.

Bangladesh Bank (2018). Annual Report July 2017–June 2018. Bangladesh Bank, Dhaka.

Bansal, P. (2005). Evolving sustainably: a longitudinal study of corporate sustainable development. *Strategic Management Journal* **26**(3), 197–218 (https://doi.org/10.1002/smj.441).

Belal, A. R., and Cooper, S. (2011). The absence of corporate social responsibility reporting in Bangladesh. *Critical Perspectives on Accounting* **22**(7), 654–667 (https://doi.org/10.1016/j.cpa.2010.06.020).

Belal, A. R., Mazumder, M. M. M., and Ali, M. (2019). Intellectual capital reporting practices in an Islamic bank: a case study. *Business Ethics: A European Review* **28**(2), 206–220 (https://doi.org/10.1111/beer.12211).

Beretta, S., and Bozzolan, S. (2004). A framework for the analysis of firm risk communication. *International Journal of Accounting* **39**(3), 265–288 (https://doi.org/10.1016/j.intacc.2004.06.006).

Berkman, H., Jona, J., Lee, G., and Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy* **37**(6), 508–526 (https://doi.org/10.1016/j.jaccpubpol.2018.10.003).

Blanc, R., Cho, C. H., Sopt, J., and Branco, M. C. (2019). Disclosure responses to a corruption scandal: the case of Siemens AG. *Journal of Business Ethics* **156**(2), 545–561 (https://doi.org/10.1007/s10551-017-3602-7).

Bodin, L. D., Gordon, L. A., Loeb, M. P., and Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy* **37**(6), 527–544 (https://doi.org/10.1016/j.jaccpubpol.2018.10.004).

Bose, S., Bhattacharyya, A., and Islam, S. (2016). Dynamics of firm-level financial inclusion: empirical evidence from an emerging economy. *Journal of Banking and Finance Law and Practice* **27**(1), 47–68.

Byron, R. K. (2016). BB installing monitoring software. *Daily Star*, March 13. URL: https://www.thedailystar.net/frontpage/bb-installing-monitoring-software-790378.

Byron, R. K., and Chakma, J. (2019). Recapitalisation of state banks: govt to inject another Tk 1,500cr. *Daily Star*, May 29. URL: https://www.thedailystar.net/business/banking/news/govt-inject-another-tk-1500cr-1750240.

Byron, R. K., and Rahman, M. F. (2016). Involvement of BB officials in cyber heist: Farashuddin wants further probe. *Daily Star*, June 9. URL: https://www.thedailystar.net/frontpage/farashuddin-wants-further-probe-1236697.

Campbell, J. L. (2007). Why would corporations behave in socially responsible ways? An institutional theory of corporate social responsibility. *Academy of Management Review* **32**(3), 946–967 (https://doi.org/10.5465/amr.2007.25275684).

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H.-M., and Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies* **19**(1), 396–455 (https://doi.org/10.1007/s11142-013-9258-3).

Chaney, P. K., Faccio, M., and Parsley, D. (2011). The quality of accounting information in politically connected firms. *Journal of Accounting and Economics* **51**(1), 58–76 (https://doi.org/10.1016/j.jacceco.2010.07.003).

Cho, C. H. (2009). Legitimation strategies used in response to environmental disaster: a French case study of Total SA's *Erika* and AZF incidents. *European Accounting Review* **18**(1), 33–62 (https://doi.org/10.1080/09638180802579616).

Daily Star (2016). $101M cyber heist: Govt probe hints at BB officials' links. *Daily Star*, May 31. URL: https://www.thedailystar.net/backpage/govt-probe-hints-bb-officials-links-1232086.

Deegan, C., Rankin, M., and Voght, P. (2000). Firms' disclosure reactions to major social incidents: Australian evidence. *Accounting Forum* **24**(1), 101–130 (https://doi.org/10.1111/1467-6303.00031).

Deephouse, D. L. (1999). To be different, or to be the same? It's a question (and theory) of strategic balance. *Strategic Management Journal* **20**(2), 147–166 (https://doi.org/10.1002/(SICI)1097-0266(199902)20:2%3C147::AID-SMJ11%3E3.0.CO;2-Q).

DiMaggio, P., and Powell, W. W. (1983). The iron cage revisited: collective rationality and institutional isomorphism in organizational fields. *American Sociological Review* **48**(2), 147–160 (https://doi.org/10.2307/2095101).

Elamer, A. A., Ntim, C. G., and Abdou, H. A. (2020). Islamic governance, national governance, and bank risk management and disclosure in MENA countries. *Business and Society* **59**(5), 914–955 (https://doi.org/10.1177/0007650317746108).

Elshandidy, T., and Neri, L. (2015). Corporate governance, risk disclosure practices, and market liquidity: comparative evidence from the UK and Italy. *Corporate Governance: An International Review* **23**(4), 331–356 (https://doi.org/10.1111/corg.12095).

Elshandidy, T., and Shrives, P. J. (2016). Environmental incentives for and usefulness of textual risk reporting: evidence from Germany. *International Journal of Accounting* **51**(4), 464–486 (https://doi.org/10.1016/j.intacc.2016.10.001).

Elshandidy, T., Fraser, I., and Hussainey, K. (2013). Aggregated, voluntary, and mandatory risk disclosure incentives: evidence from UK FTSE all-share companies. *International Review of Financial Analysis* **30**, 320–333 (https://doi.org/10.1016/j.irfa.2013.07.010).

Faccio, M. (2006). Politically connected firms. *American Economic Review* **96**(1), 369–386 (https://doi.org/10.1257/000282806776157704).

Financial Reporting Council (2016). Summary of key developments for 2016 annual reports. Summary, FRC, London. URL: https://bit.ly/3nJG04A

Ghafur, A. (1976). On the nationalised industrial sector controversy. *Political Economy: Journal of Bangladesh Economic Association* **2**(1), 5–10.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Sohail, T. (2006). The impact of the Sarbanes–Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy* **25**(5), 503–530 (https://doi.org/10.1016/j.jaccpubpol.2006.07.005).

Gordon, L. A., Loeb, M. P., and Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly* **34**(3), 567–594 (https://doi.org/10.2307/25750692).

Hammer, J. (2018). The billion-dollar bank job. *New York Times Magazine*, Money Issue, May 3. URL: https://nyti.ms/2KKtSRW.

Haniffa, R., and Hudaib, M. (2007). Exploring the ethical identity of Islamic banks via communication in annual reports. *Journal of Business Ethics* **76**(1), 97–116 (https://doi.org/10.1007/s10551-006-9272-5).

Hermit, W. (2020). Difference between the determinants of operational risk reporting in Islamic and conventional banks: evidence from Saudi Arabia. *The Journal of Operational Risk* **15**(1), 49–86 (https://doi.org/10.21314/JOP.2019.235).

Hofileña, J. M. G., and Sy, J. L. (2017). Gone without a trace: a re-examination of bank secrecy laws and anti-money laundering laws in light of the 2016 Bangladesh bank heist. *Ateneo Law Journal* **62**, 90–139.

Holt, T. J., and Kilger, M. (2012). Examining willingness to attack critical infrastructure online and offline. *Crime and Delinquency* **58**(5), 798–822 (https://doi.org/10.1177/0011128712452963).

Institute of Chartered Accountants of England and Wales (2018). Audit insights: cybersecurity: coping with increasing complexity. Report, Institute of Chartered Accountants of England and Wales (ICAEW), London. URL: https://bit.ly/3nEVIOj.

Kashmiri, S., Nicol, C. D., and Hsu, L. (2017). Birds of a feather: intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science* **45**(2), 208–228 (https://doi.org/10.1007/s11747-016-0486-5).

Lange, R., and Burger, E. W. (2017). Long-term market implications of data breaches, not. *Journal of Information Privacy and Security* **13**(4), 186–206 (https://doi.org/10.1080/15536548.2017.1394070).

Li, F. (2010). Survey of the literature. *Journal of Accounting Literature* **29**, 143–165.

Li, H., and Zhang, Y. (2007). The role of managers' political networking and functional experience in new venture performance: evidence from China's transition economy. *Strategic Management Journal* **28**(8), 791–804 (https://doi.org/10.1002/smj.605).

Li, H., No, W. G., and Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems* **30**, 40–55 (https://doi.org/10.1016/j.accinf.2018.06.003).

Lim, A., and Tsutsui, K. (2012). Globalization and commitment in corporate social responsibility: cross-national analyses of institutional and political-economy effects. *American Sociological Review* **77**(1), 69–98 (https://doi.org/10.1177/0003122411432701).

Linsley, P. M., and Shrives, P. J. (2006). Risk reporting: a study of risk disclosures in the annual reports of UK companies. *British Accounting Review* **38**(4), 387–404 (https://doi.org/10.1016/j.bar.2006.05.002).

Marquis, C., and Qian, C. (2014). Corporate social responsibility reporting in China: symbol or substance? *Organization Science* **25**(1), 127–148 (https://doi.org/10.1287/orsc.2013.0837).

Mazumder, M. M. M., and Hossain, D. M. (2019). Exploring the nature of risk disclosure in the annual report narratives of Bangladeshi pharmaceutical companies: an impression management perspective. *International Journal of Comparative Management* **2**(3), 273–296 (https://doi.org/10.1504/IJCM.2019.105975).

Meyer, J. W., and Rowan, B. (1977). Institutionalized organizations: formal structure as myth and ceremony. *American Journal of Sociology* **83**(2), 340–363 (https://doi.org/10.1086/226550).

Milne, M. J., and Adler, R. W. (1999). Exploring the reliability of social and environmental disclosures content analysis. *Accounting, Auditing and Accountability Journal* **12**(2), 237–256 (https://doi.org/10.1108/09513579910270138).

Morse, E. A., Raval, V., and Wingender, J. R., Jr. (2017). SEC cybersecurity guidelines: insights into the utility of risk factor disclosures for investors. *Business Lawyer* **73**(1), 1–34.

Muttakin, M. B., Mihret, D. G., and Khan, A. (2018). Corporate political connection and corporate social responsibility disclosures. *Accounting, Auditing and Accountability Journal* **31**(2), 725–744 (https://doi.org/10.1108/AAAJ-06-2015-2078).

Nelson, K. K., and Pritchard, A. C. (2016). Carrot or stick? The shift from voluntary to mandatory disclosure of risk factors. *Journal of Empirical Legal Studies* **13**(2), 266–297 (https://doi.org/10.1111/jels.12115).

Nobanee, H., and Ellili, N. (2016). Corporate sustainability disclosure in annual reports: evidence from UAE banks: Islamic versus conventional. *Renewable and Sustainable Energy Reviews* **55**, 1336–1341 (https://doi.org/10.1016/j.rser.2015.07.084).

Nuruzzaman, M. (2004). Neoliberal economic reforms, the rich and the poor in Bangladesh. *Journal of Contemporary Asia* **34**(1), 33–54 (https://doi.org/10.1080/00472330480000291).

Okhmatovskiy, I. (2010). Performance implications of ties to the government and SOEs: a political embeddedness perspective. *Journal of Management Studies* **47**(6), 1020–1047 (https://doi.org/10.1111/j.1467-6486.2009.00881.x).

Oliveira, J., Rodrigues, L. L., and Craig, R. (2011). Risk-related disclosures by non-finance companies. *Managerial Auditing Journal* **26**(9), 817–839 (https://doi.org/10.1108/02686901111171466).

Oliver, C. (1991). Strategic responses to institutional processes. *Academy of Management Review* **16**, 145–79 (https://doi.org/10.5465/amr.1991.4279002).

Pache, A. C., and Santos, F. (2010). When worlds collide: the internal dynamics of organizational responses to conflicting institutional demands. *Academy of Management Review* **35**, 455–76 (https://doi.org/10.5465/amr.35.3.zok455).

Rahman, M. F., and Khan, T. (2012). A question of public trust. *The STAR: A Weekly Publication of the Daily Star* **11**(27). URL: https://www.thedailystar.net/magazine/2012/09/03/cover.htm.

Rao, H., Morrill, C., and Zald, M. N. (2000). Power plays: how social movements and collective action create new organizational forms. *Research in Organizational Behavior* **22**, 237–81 (https://doi.org/10.1016/S0191-3085(00)22007-8).

Richardson, V. J., Smith, R. E., and Watson, M. W. (2019). Much ado about nothing: the (lack of) economic impact of data privacy breaches. *Journal of Information Systems* **33**(3), 227–265 (https://doi.org/10.2308/isys-52379).

Ruef, M., and Scott, W. R. (1998). A multidimensional model of organizational legitimacy: hospital survival in changing institutional environments. *Administrative Science Quarterly* **43**, 877–904 (https://doi.org/10.2307/2393619).

Saggar, R., and Singh, B. (2017). Corporate governance and risk reporting: Indian evidence. *Managerial Auditing Journal* **32**(4), 378–405 (https://doi.org/10.1108/MAJ-03-2016-1341).

Scott, W. R. (2014). *Institutions and Organizations: Ideas, Interests and Identities*, 4th edn. Sage, Thousand Oaks, CA.

Securities and Exchange Commission (2011). Cybersecurity. CF disclosure guidance: topic no 2. Report, October 13, Division of Corporation Finance, SEC. URL: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Shibli, A. (2016). The Bangladesh Bank heist: need for better systems and protocols. *Daily Star*, March 14. URL: https://www.thedailystar.net/op-ed/politics/need-better-systems-and-protocols-790702.

Shipilov, A. V., Greve, H. R., and Rowley, T. J. (2010). When do interlocks matter? Institutional logics and the diffusion of multiple corporate governance practices. *Academy of Management Journal* **53**, 846–64 (https://doi.org/10.5465/amj.2010.52814614).

Sobhan, A. (2016). Where institutional logics of corporate governance collide: overstatement of compliance in a developing country, Bangladesh. *Corporate Governance: An International Review* **24**(6), 599–618 (https://doi.org/10.1111/corg.12163).

Sobhan, A., and Bose, S. (2019). Institutional characteristics and outcomes of corporate governance in Bangladesh: research challenges. In *The Routledge Companion to Accounting in Emerging Economies*, Tsalavoutas, I., and Weetman, P. (eds), Chapter 16. Taylor and Francis, Oxford (https://doi.org/10.4324/9781351128506).

Sobhani, F. A., Amran, A., and Zainuddin, Y. (2012). Sustainability disclosure in annual reports and websites: a study of the banking industry in Bangladesh. *Journal of Cleaner Production* **23**(1), 75–85 (https://doi.org/10.1016/j.jclepro.2011.09.023).

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review* **20**(3), 571–610 (https://doi.org/10.5465/amr.1995.9508080331).

Unerman, J. (2000). Methodological issues: reflections on quantification in corporate social reporting content analysis. *Accounting, Auditing and Accountability Journal* **13**(5), 667–680 (https://doi.org/10.1108/09513570010353756).

US Department of Justice (2018). Criminal complaint to United States District Court for the Central Court of California. Document, US District Court. URL: https://www.justice.gov/opa/press-release/file/1092091/download.

Wang, Q., Wong, T. J., and Xia, L. (2008). State ownership, the institutional environment, and auditor choice: evidence from China. *Journal of Accounting and Economics* **46**(1), 112–134 (https://doi.org/10.1016/j.jacceco.2008.04.001).

Wang, T., Kannan, K. N., and Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research* **24**(2), 201–218 (https://doi.org/10.1287/isre.1120.0437).

Zhang, L., Xu, Y., Chen, H., and Jing, R. (2020). Corporate philanthropy after fraud punishment: an institutional perspective. *Management and Organization Review* **16**(1), 33–68 (https://doi.org/10.1017/mor.2019.41).