Cyber Security disclosure in the banking sector: A case of South Africa and China

Mr Frans Duvenhage[1,*], Prof Anet Smit[2], Dr Martin Botha[3]

[1] MBA student, NWU Business School, North-West University, Potchefstroom, South Africa

[2] NWU Business School, North-West University, Potchefstroom, South Africa

[3] Faculty of Economic and Management Sciences, North-West University, Potchefstroom, South Africa

Keywords

Cyber risk; Financial sector; Disclosure

Abstract

This study compares risk reporting, specifically cyber risk reporting, between South African and Chinese banks. Major corporate scandals had significant impacts on the economic environment and has led to an increased interest in risk reporting. The population is all the listed financial service providers (banks) in South Africa and China. By purposeful sampling the four biggest banks in each country were selected based on their asset value. The research method utilised is content analysis. A disclosure index is developed from the literature study and used to analyse the results. It is concluded that the disclosure practices on cyber risks of the banks differ substantively between the two countries. China does not explicitly refer to cyber risk but only discloses it as an operational risk in its annual reports. No ranking is associated with any of their risks or categories. This is in contrast when compared to the South African annual reports as South African banks clearly define cyber risk and rank it amongst their top risks.

1. Introduction

All Stock Exchange-listed companies must publish their annual financial results (Khlif, Ahmed, Souissi & Sargsyan, 2018). The financial part of the disclosures is more regulated than some of the non-financial disclosures. Since the non-financials are not as regulated, organisations struggle to navigate the sometimes-confusing landscape of disclosure where numerous frameworks and standards exist (Elshandidy, Shrives, Bamber & Abraham, 2018:2; Krzus, 2011). The Securities and Exchange Commission ("SEC") is very concerned about cyber risk. In February 2018, the SEC updated the 2011 guidelines and stated that public businesses must stay focused on cybersecurity issues and take all required efforts to inform investors about

*Corresponding Author

[1] Frans.duvenhage@gmail.com

[2] Anet.smit@nwu.ac.za

[3] Martin.botha @nwu.ac.za

substantial cybersecurity risks and events. Under the Securities Act of 1933 and Securities Exchange Act of 1934, corporations must report their cyber controls, risks, and vulnerabilities (SEC, 2018 & SECPCCD, 2018). While banking law and regulation have been inactive in the face of cyber risk, the SEC has made some progress. Skinner (2019) critically examined nearly 900 SEC filings filed by seven prominent U.S. bank holding corporations during a three-year period that are covered by the framework of mandatory disclosures. Their review suggests that SEC laws and recommendations are too broad for these institutions, and not enough to address public and private interests. The study, therefore, urges the SEC to adopt more nuanced cyber disclosure standards for banks. It is evident from the prior evidence (Skinner, 2019) that, the SEC has led among financial regulators in addressing cyber risk, primarily through a focus on disclosure.

From a societal standpoint, cyber risk is especially concerning when it comes to systemically important financial institutions, such as the largest internationally active banks. This is because the overall stability of the financial system and thus the real economy depends on these banks' ability to withstand stressful events such as cyber-attacks. The main aim of this paper is to analyse the degree of cyber risk disclosure in the banking sector and compare cyber risk disclosure practises in the banking sector in South Africa and China.

Risk is vital to any organisation, and businesses must identify, evaluate, manage, and report all types of risk to enhance decision-making (CIMA, 2008). Risk is one of the leading causes of uncertainty in an organisation and can originate from various internal and external sources (Epstein & Rejc, 2006). Risk management can be associated with two types of events: risks or adverse events and opportunities or positive events (Ata & Schmandt, 2016).

Most investors prefer principal risk reporting that is specific to an organisation. They need improved disclosure that avoids boilerplate text and provides enough detail to understand how the organisation accounts for its transactions, how it identified its principal risks and how the organisation is planning to manage those risks (Financial Reporting Council (FRC), 2017:3). Management can improve investor confidence if they can prove how the reported risks relate to the business model (FRC, 2017). As stated in a recent study by Gao, Calderon & Tang (2020) cybersecurity risks are important and could affect business operations and the integrity of financial reporting, although there is limited empirical research on the cybersecurity risk disclosures. The following section will highlight related aspects to provide more background on cyber risk disclosure in the banking sector.

2. Background to the study

The 2007 global financial crisis was partly due to most of the banks lacking the ability to combine their risk exposures and identify risk concentrations at a bank group level (Thun, 2015). As a result, more banks are starting to identify cyber risk as a priority risk (Härle, Havas, Kremer, Rona & Samandari, 2016:4). Furthermore, as technology and digital banking has developed in the past decade, cyber risk, and the need to disclose information has escalated.

To support the quality disclosure of information, various reporting guidelines and frameworks have been developed. All listed South African companies are required by the Johannesburg Securities Exchange (JSE)

to comply with the International Financial Reporting Standards (IFRS) as well as the King reports (IODSA, 2010; JSE, 2017). King III report was the first report that stated that organisations need to produce an integrated report instead of both a traditional annual financial and a sustainability report. King III declares that listed organisations that fail or choose not to produce integrated reports must explain why they are not adhering to this requirement (IODSA, 2010).

Integrated reporting states that organisations should disclose the specific risks they face, what possible opportunities can arise from these risks, and how they affect the organisation's ability to create value (Integrated Reporting Committee of South Africa, 2018). To regulate and improve security, listed companies must adhere to some listing requirements. King IV outlines the requirements for risk governance in principle 11, which states: "The governing body should govern risk in a way that supports the organisation in setting and achieving its strategic objectives" (IODSA, 2016). King IV provides a series of recommended risk practices that the governing body of any listed organisation should perform.

3. Problem Investigated

In the business world, business risks have always existed. In addition, there have been major corporate scandals that had significant impacts on the economic environment. All of which has led to an increased interest in risk reporting (Oliveira, Rodrigues & Craig, 2013). It became clear that some banks manage their risks poorly due to weak risk data compiling capabilities and risk reporting practices. The poor management of risks proved to have severe consequences on the banks themselves and the financial system's stability (Bank for International Settlements (BIS), 2013).

In a study done by Linsley and Shrives (2000), they argue that organisations have become more exposed to volatility and uncertainties (Khlif & Hussainey, 2016:181). Although there have been many improvements in recent years, investors still know too little about an organisation's risks, and a risk information gap still exists between organisations and their stakeholders (Wilson, 2014). In addition, it was found that organisations are reluctant to comply with risk disclosure requirements (Al-Hadi, Hasan & Habib, 2016). In general, larger organisations are more complex and have a more comprehensive range of operations. Therefore, the statement above implies that they are subject to higher risk levels, translating into higher information irregularities amongst investors (Al-Hadi et al., 2016).

Media platforms report daily on the rampant increase in cybercrime. This increase has sparked fear in the public eye that cyberattacks would affect national resources and destabilise infrastructure (Berry, 2018). One of the main contributing factors to this naivety is that the Protection of Personal Information Act (POPIA) is not entirely in effect. Sophos, an organisation that is a global leader in network security, conducted a study and found that only 34% of South African organisations comply with the POPI Act (Sophos, 2019). Every day, media organisations report on the unprecedented growth in cybercrime. This increase has raised widespread concern that cyberattacks will harm national resources and impair infrastructure (Berry, 2018).

Between January and August 2018, South African Banking Risk Information Centre (SABRIC) reported that an estimated R250 million were lost due to cyber and digital banking crimes. However, these losses

are only the reported statistics. Most cybercrimes go unreported (SABRIC, 2019). Furthermore, as discussed in the problem statement, it seems that risk disclosures in general, but cyber risks specifically, are not reported uniformly between organisations, leading to this study's objective.

4. Research Objectives

The main objective of this paper is to evaluate the level of disclosure on cyber risk in the banking sector and compare the practices of cyber risk disclosure in the banking sector between South Africa and China.

4.1 Secondary Objectives

The secondary objectives include the following:

To identify the rules and regulations that govern reporting disclosures in South Africa and China.

To identify the research method and the sources of the data.

To develop the measuring instrument and to analyse the data.

5. Literature Review

5.1. Risk reporting

Risk reporting tends to be more non-financial than financial information, historical rather than future-orientated, and qualitative rather than quantitative. The current reporting shortcomings have emphasised the need for a more integrated and holistic form of reporting that will integrate both the financial and non-financial information in a meaningful and integrated manner (Carels, 2014:3; Global Reporting Initiative (GRI), 2018)

Elshandidy and Neri (2015) postulate that organisations, in general, do not tend to provide quantitative and forward-looking attributes related to risk disclosure but qualitative and historical information. Variations in risk disclosure are partially aligned with country-related regulations, which plays a vital role in an organisations incentive. The impacts of risk factors vary by country. In the United States and Canada, an organisation's risk disclosure is positively associated with its risk levels. In contrast, German organisations are negatively associated with their risk levels, and United Kingdom organisations are not significantly related (Elshandidy *et al*., 2018). Cyber risk is identified as the fourth most crucial risk out of ten identified by Corporate Compliance Insights (CCI), Deloach, 2019).

5.2. Regulatory requirements for risks reporting

To regulate and improve security, listed companies must adhere to some listing requirements. Organisations must comply with International Financial Reporting Standards (IFRS) (JSE, 2017). As per principal 7 of IFRS, organisations are required to list the nature and extent of risks arising from financial instruments to which the entity is exposed during the period and at the end of the reporting period, and how the entity manages those risks. The qualitative disclosures describe management’s objectives, policies, and processes for managing those risks, and need to be included (IFRS, 2018). All listed organisations in South Africa must comply with King IV and IFRS as stipulated in the JSE listing requirements.

China’s financial reporting had to adhere to all the requirements as stipulated by China Accounting Standards Committee (CASC) until China adopted accounting standards specified by the International Accounting Standards Board (IASB) (CASC, 2018). The Chinese Accounting Standards (CAS) were replaced by the International Financial Reporting Standards (IFRS). This replacement brings China more in line with the rest of the world. The new procedures became law on 1 January 2007. China complies with various IFRS standards, specifically IFRS 7, as stated above. IFRS 7 requires entities to provide disclosure in their financial statements that enable users to evaluate the significance of financial instruments and the risks arising from these financial instruments (IFRS, 2018). This practice is like the South African reporting requirements as stipulated by the JSE.

5.3 Risks reporting in the financial sector

The China Banking Regulatory Commission (CBRC) adopted regulations that came into effect on 1 January 2013. According to these regulations, all China's commercial banks are required to disclose information related to exposure and evaluation of credit risk, operational risk, market risk and any other relevant risks, as well as risk management (Wang, Chen & Zhao, 2018:2).

After the global financial crisis that started in 2007, a key finding was that information technology and data architecture in the banking sector was severely lacking and unable to support the broader management with financial risks (BIS, 2013:8). As a result, most banks could not combine their risk exposures and detect risk concentrations quickly and accurately at a bank group level, across business lines and between legal entities (Thun, 2015). Some banks managed their risks poorly due to weak risk data compiling capabilities and risk reporting practices. The poor management and availability of data proved to have severe consequences to the banks themselves and the financial system's stability (BIS, 2013).

5.4 Cyber risks in the banking sector

Organisations depend more and more on digital technology to conduct their business operations and use digital technology to engage with their customers, business partners, and other constituencies (Securities & Commission, 2018:2). This technological advancement and digital connection in the world have presented some risks. Cybersecurity is an ever-present ongoing risk to all markets and industries (Securities & Commission, 2018). As the banking sector is highly advanced in technology and relies on digital connections, the sector is vulnerable in terms of cyber risk (Bouveret, 2018). After the release of the Securities and Exchange Commission's (SEC's) cybersecurity disclosure guidance in October 2011, cybersecurity risk disclosure has been intensified according to Li, No & Wang (2018). They investigate the usefulness of cybersecurity-related risk factors disclosed in 10-K filings and subsequently reported that SEC’s disclosure guidance encourages firms to increase their disclosure of cybersecurity risks (Li, No & Wang, 2018).

Businesses are primarily concerned, as cyber-attacks could lead to substantial costs and various other implications such as exposure of sensitive personal information, business disruptions, and remediating costs. Other expenses such as increased cybersecurity protection cost, litigation and legal risk, reputational

damage could also occur. (Li, No & Wang, 2018:40; Securities & Commission, 2018:4). In 2018 cybersecurity played a vital role in the Securities and Exchange Commission's (SEC) regulatory agenda. The commission published an interpretive guideline that urges companies to be: "more transparent in disclosing cybersecurity risks in their public filings and to disclose material data security incidents in a timely fashion. In addition, the SEC urges businesses to implement safeguards such as trading bans to prevent insiders from selling securities after a breach is detected but before it is publicly disclosed" (Newman & Belknap, 2019).

Cyber risk can be defined as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems" (Bouveret, 2018). Eling & Wirfs (2016) add to this definition by mentioning that cyber risk shares similar property and liability risk characteristics as catastrophic and operational risk. Cyber-attacks have a severe impact, directly and indirectly, on an organisation, and losses occurred from cyber breaching be significant (Bouveret, 2018). In a study done by Cavusoglu, it was established that a cybersecurity breach could negatively affect an organisation's share price by up to two and a half per cent (Eling & Schnell, 2016:477). However, not all cyber risks are related to cyber-attacks or "hacks" that are malicious, and some occur due to business disruptions such as software updates. These are referred to as cyber incidents (Bouveret, 2018). Business disruptions hinder organisations from operating, resulting in lost revenue, while the effects of data breaches materialise over a more extended period. All these causes reputational damage and possible litigation costs (Bouveret, 2018:4). In addition, the loss of confidence following a cyber-attack could be significant for the financial sector, given the reliance of financial institutions on the trust of their customers (Warren, Kaivanto & Prince, 2018:28).

Based on the literature study, a measuring instrument was developed to measure the disclosures of the different banks. The paper addresses the disclosure practices of the banks on cyber risks in a systematic way by dividing the information into different sections, namely General information, Governance of risks, ranking of cyber risks, Reporting on cyber risk incidents, Causes of cyber risks, The impact of cyber risks incidents and the overall level of disclosure. These sections correspond with the layout of the disclosure index, as displayed in Table 1. In the next paragraphs are brief discussion on each section.

- ***Governance of risk***

Any organisation needs to have policies and procedures in place to manage its risks. For example, government Gazette, No. 35950, sub-regulation 17 states the following: "achieves the objectives relating to sound corporate governance and effective risk management and complies with the relevant minimum requirements specified in regulation 39". This regulation covers managing risk management processes, managing material exposures to risk, and reporting material information technology and cyber incidents (SARB, 2012; SARB, 2019). As per Principle 11 of King IV: "The governing body should govern risk in a way that supports the organisation in setting and achieving its strategic objectives" (IODSA, 2016:61). This principle entails that the governing body assigns implementation and risk management responsibility

to a responsible individual. Risks need to be managed as an integral part of the company's day to day activities (IODSA, 2016:61).

The cybersecurity law in China came into force on 1 June 2017. Under the cybersecurity law network, operators are required to appoint a designated person in charge of cybersecurity. To identify responsible people or directors with expertise in the field of cybersecurity, was evident in a study by Klemash, Smith & Seets (2020) which indicates that 58% of the Fortune 100 companies included cybersecurity as an area of expertise sought on the board. In addition, all cybersecurity incidents must be monitored and recorded (Ning & Wu, 2019). In table 1, below, six questions need to be evaluated to analyse the governance of risks.

- ***Ranking of cyber risk***

Organisations such as Forbes and the World Economic Forum lists cyber risk as one of the top 10 risks (Demrovsky, 2019; Fleming, 2019). Business tech ranks cybersecurity as ninth in the listed risks affecting the South African economy (Businesstech, 2019). Laws in China regulating cyber risks were only implemented in 2017. Therefore, there is no clear indicator of whether cyber risk is ranked in the Chinese business environment (KPMG, 2017:4). The literature above is proficient at investigating how the banks rate the importance of cyber risk. The "Ranking of cyber risk" section, as in table 1, addresses the following two questions:

- Does the bank rate cyber risk as one of its top ten risks?
- If ranked, how important are cyber risks to the bank?

- ***Reporting of cyber risk incidents***

The South African Reserve Bank has issued a new directive 2/2019 regarding Regulation 39 on the regulations relating to the Banks Act 94 of 1990. The directive sets out the reporting requirements for cyber incidents. The Protection of Personal Information Act (POPIA) was introduced in 2013. After it comes into full effect, section 22 of POPIA requires that any data breach or suspected breach be reported to the information regulator and the affected parties. Under the Cyber Crimes Act, the incident must be reported within 72 hours.

Following the Chinese Cybersecurity Law, organisations must notify the relevant authorities of any cyber incidents within 24 hours. If the publication of such an event will jeopardise China's national security, then such information will be withheld. In addition, as with the POPI Act, Chinese Cybersecurity Law requires organisations to notify affected users in case of disclosure and damage or loss of user information. Currently, relevant laws and regulations in China do not provide specific requirements about the nature and scope of information to be reported. This practice is similar to King IV, where there are no precise reporting requirements and limited guidance for reporting cyber incidents. Therefore, the following question is considered in this section on "Reporting of cyber risk incidents":

- Identify if there was a cyber risk incident, was this cyber risk incident reported?

- ***Causes of cyber risk incidents***

Banks face many cybersecurity threats that fall within these three categories (Tylor, 2018), namely Financial gain, Disruption and Espionage. Virtually every cyber threat can be categorised into one of these three types. With current technology, there is an abundance of methods to initiate an attack. The results of a study performed by Gao, Calderon & Tang (2020) show that the two most disclosed cybersecurity risks are risks of service/operation disruption and risks of data breach. Below is a list of the ten most common types of cyber threats: Malware, Phishing, Spear Phishing, "Man in the Middle" (MitM) attack, Trojans, Ransomware, Denial of Service Attack or Distributed Denial of Service Attack (DDoS), Attacks on Internet of Things (IoT) Devices Data Breaches and Malware on Mobile Apps. (Regan, 2019, Norten, a-f, 2019). In table 1, the banks are analysed accordingly.

- **T*he impact of cyber risk incidents***

A successful cyber-attack can cause severe damage to an organisation. It impacts an organisation's bottom line, the organisation's standing and consumer trust. The impact of a cyber-attack can be divided into three categories (Cruickshank, 2019) which are considered in the disclosure index:

  - Damage to the reputation
  - Financial losses
  - Legal actions or implications.

- ***Mitigating procedures***

A risk mitigation strategy is an action plan that organisation create after they have made a thorough evaluation of possible threats that can affect the organisation. The purpose of such a strategy is to minimise or ideally prevent adverse impact before any damage or disaster takes place (Cantoria, 2019). Therefore, the following question is considered:

  - Is a mitigation procedure in place?

- ***Level of disclosure***

The level of disclosure aims to display how much information each organisation discloses on cyber risk. However, previous studies have raised concerns on the unit of analysis used to determine the amount of disclosure even though it is common practice to use words or sentences (Amran, Bin & Hassan, 2009). For example, Linsley & Shrives (2006) argued that it is difficult to determine which words can be used to estimate risk disclosure. However, early studies done by Hackston & Milne (1996) and later copied by Linsley & Shrives (2006) indicate using either sentences, words, graphs, or columns all similar yield results. Therefore, for this study, a word search for all cyber-related phrases was done to determine the level of disclosure.

6. Research Methodology

The research method utilised is content analysis. A disclosure index is developed from the literature studied. Finally, the disclosure index is used to analyse the results. The population is all the listed financial service providers (banks) in South Africa and China. The sampling method used is purposeful sampling, where a particular setting is explicitly selected for the information, it can provide (Bryman & Bell, 2014). The banks were selected based on their asset value. China was chosen as it is an emerging economy, and along with South Africa, it is part of the BRICS countries (Asongu, Akpan & Isihak:2018:2).

For the South African market, the four biggest banks were selected based on their asset value. These four banks (FirstRand Bank, Standard Bank, Absa Bank, Nedbank) had a combined asset value of 5 940.6 billion rands in 2018 (454.1 billion dollars) (Businesstech, 2018). In 2017 FirstRand had the most significant headline earnings of 22.4 billion rands, and Standard bank has the most extensive footprint of all the South African banks (Businesstech, 2017). These banks represented most of the South African banking sector and will remove the possibility of the much smaller banks skewing the findings (Bryman & Bell, 2014).

For the Chinese financial markets, the following four banks in China were selected based on their asset value – the Industrial and Commercial Bank of China, China Construction Bank, Bank of China, and the Agricultural Bank of China. These are the four biggest banks in China, having a combined asset value of 13 637.2 billion dollars (Businesstech, 2018), and according to the British magazine "The Banker", these banks are also the four biggest banks in the world (Businesstech, 2018; chinaplus.cri.cn, 2018). The four banks from the South African market and the four banks from the Chinese market give a total sample size of eight units. All the banks chosen for this study must submit annual financial reports as stipulated by the JSE and CASC (CASC, 2018; JSE, 2017). These annual reports are available for download online. Following the discussion on the research methodology, details concerning the disclosure index are displayed in the next section.

6.1 Disclosure index

The disclosure index is built around the reporting requirements indicated by the IIRC and CASC and the Chinese Cybersecurity Law requirements. Therefore, this study is systematic and fully replicable. As shown in Table 1, the disclosure index is used to measure the disclosure practices of the banks. The numeric values assigned are derived from the observations of the index. For example, should something be true, or "Yes", a numeric value of 1 would be assigned to that observation? Should something be false, or "No", a numeric value of 0 would be assigned. If no value could be assigned due to the criteria not being met, the field was assigned a not applicable (N/A). Table 1 is the presentation of the measured criteria from each of the banks' annual reports.

Table 1: Cyber risk disclosure index

	FirstRand	Standard Bank	Absa Bank	Nedbank	Industrial & Commercial Bank of China	China Construction Bank	Bank of China	Agricultural Bank of China
General information								
Does the bank produce an integrated report (Yes/No?)	Yes	Yes	Yes	Yes	No	No	No	No
Which rules and regulations does the bank adhere to:								
IFRS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
KING IV	Yes	Yes	Yes	Yes	No	No	No	No
Is cyber risk reporting mandatory?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Governance of risk								
Does the bank have a policy on risks reporting in general?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Does the bank have a cyber risk policy?	Yes	No	Yes	Yes	No	No	No	No
Does the board of the bank take ownership?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do they refer to any strategy related to managing cyber risks?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Does the bank define cyber risk clearly?	Yes	No	Yes	Yes	No	No	No	No
Does the bank identify cyber risk as a material item?	No	Yes	Yes	Yes	No	No	No	No
Ranking of cyber risk								
Does the bank rank cyber risk as one of its top ten risks?	No	No	Yes	Yes	No	No	No	No
If ranked, how important are cyber risks for the bank?	N/A	N/A	1	2	N/A	N/A	N/A	N/A
Reporting of cyber risk incidents								
If there was a cyber risk incident, was the cyber risk incident reported?	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CAUSES OF CYBER RISKS INCIDENTS								
Identify the cause of the cyber risk incident.								
Malware	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Phishing	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Spear Phishing	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Man in the Middle	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Trojans	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Ransomware	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Denial of Service Attack	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Attacks on IoT devices	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Data Breaches	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Malware on mobile apps	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
The impact of cyber risk incidents								
A description of the impact on the bank:								
Damage to the reputation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Financial losses	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Legal actions or implications.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Mitigating procedures								
Is a mitigation procedure in place?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

7. Results and Findings

7.1 General information analysis

In the first place, the disclosure index starts collecting general information based on the following questions:

- Does the bank produce an integrated report?
- Rules and regulations the banks need to adhere to; and
- Are the rules of reporting cyber risks mandatory or not?

Table 2: General information analysis

General information	**Compliance Percentages**
Does the bank produce an integrated report?	50%
Which rules and regulations does the bank adhere to:	
IFRS	100%
King IV	50%
Is cyber risk reporting mandatory?	100%

When analysing the results about the general information, it is evident from Table 2 that 50% of the banks in the sample produce integrated reports. In addition, all the banks complied with IFRS reporting standards, and 50% complied with King IV regulations. These results indicated that half the banks within the total sample must comply with different reporting regulations, although all the banks must report cyber risk incidents.

7.2 Governance risk analysis

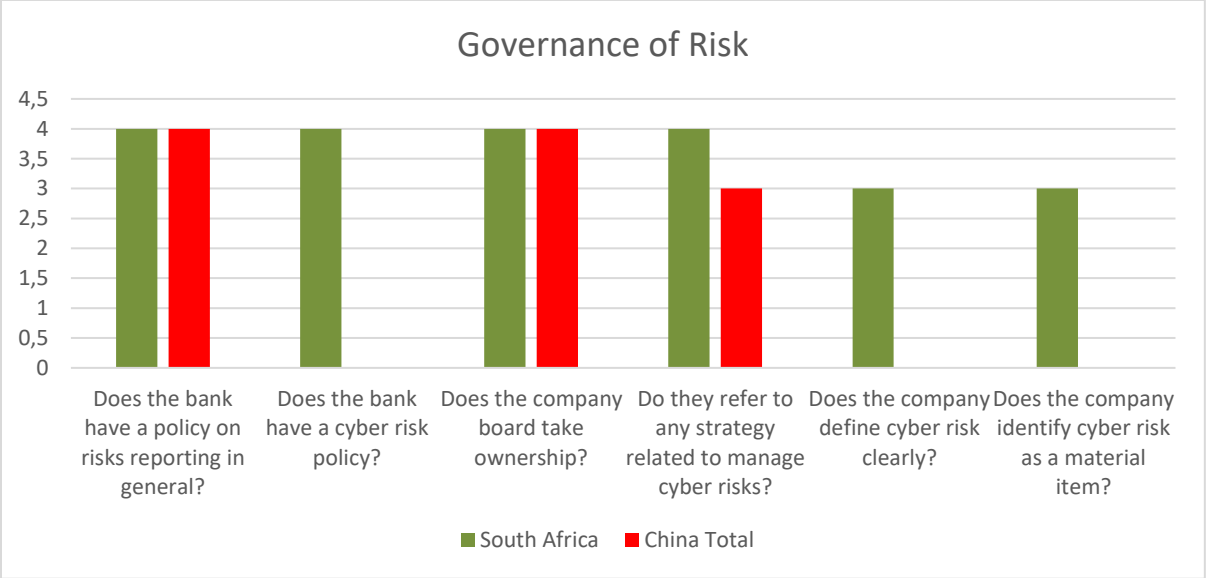
The initial steps in cyber risk management are to realise the current threats and set risk management goals (Eling & Schnell, 2016:480). Risk management has advanced to such a degree that many standards can assist in managing cyber risk. This section looks at the extent to which the banks govern risks.

Table 3: Governance risk analysis

Governance of risk	**Percentages**
Does the bank have a policy on risk reporting in general?	100%
Does the bank have a cyber risk policy?	38%
Does the board of the bank take ownership of managing risk?	100%
Do they refer to any strategy related to managing cyber risks?	88%
Does the bank define cyber risk clearly?	38%
Does the bank identify cyber risk as a material item?	38%

All the banks had a risk reporting policy, but only 38% had a cyber risk policy. Only 38% had a clear definition of cyber risk, and 88% of the banks had implemented strategies to manage cyber risk.

Additionally, 38% of the banks identified cyber risk as a material item, including Standard Bank. However, Standard Bank does not define cyber risk in its reporting. These results are conflicting and could indicate that cyber risk incidents reported by them could relate to a broader range of concerns than assumed in general. From the six questions only, Absa and Nedbank both scored 100% compliance. When addressing the governance section, the banks yielded a 67% compliance rate for the specific questions asked. Graph 1 summarises the above and illustrates it by country.



Graph 1: Governance of risk

Analysing the countries individually, China had an average compliance rate of 46%, while South Africa had almost double the percentage of 88% compliance in reporting on the governance of risks.

7.3 Ranking of cyber risk

This section looks at the cyber risk ranking within the banks.

Table 4: Ranking of cyber risk analysis

Ranking of cyber risk	Percentages
Does the bank rank cyber risk as one of its top ten risks?	25%

When analysing the risk rankings, only 25% provided a ranking for the risks they faced. However, the two banks, which provided cyber risk rankings, rated cyber risk amongst their top three risks.

7.4 Reporting of cyber risk incidents analysis

One of the SEC guidelines is that organisations disclose all prior cyber risk incidents and their impact (Newman & Belknap, 2019). This section looks at cyber risks' incidents, the causes of these incidents, and if the incidents were reported.

Table 5: Reporting of cyber risk analysis

Reporting of cyber risk incidents		**Percentages**	
If there was a Cyber risk incident, was a cyber risk incident reported?		0%	
CAUSES OF CYBER RISKS INCIDENTS			
Identify the cause of the cyber risk incident			
Malware	x	Ransomware	x
Phishing	x	Denial of Service attack	x
Spear Phishing	x	Attacks on IoT devices	x
Man in the Middle	x	Data Breaches	x
Trojans	x	Malware on mobile apps	x
What was the impact of these incidents			
A description of the impact on the bank:			
Damage to the reputation		x	
Financial losses		x	
Legal actions or implications.		x	

For the 2018 financial year, there were no cyber risk incidents confirmed in the annual reports. However, this result might be a limitation of the annual reports, and such incidents might be found in additional reports.

7.5 Mitigating procedures analysis

This section identifies if the banks have mitigation procedures in place for risks in general.

Table. 6: Mitigation procedures analysis

Are mitigating procedures in place	**Percentages**
Is a mitigation procedure in place?	100%

All the banks have stated that they do have risk mitigation procedures in place. However, very few referred explicitly to cyber risk mitigation procedures. The following section evaluates the levels of disclosure between South Africa and China in terms of cyber risk reporting.

7.6 Level of disclosure analysis

A search based on word count was done to evaluate the overall level of disclosure on cyber risk reporting. A word search was applied to evaluate how many times all related cyber terms appear in the annual reports. This includes “cyber risk”, “cyber risk”, “cybercrime”, “cyber security” and “cybersecurity” to name but a few. This section indicates the level of disclosure per bank.

Table 7: Level of disclosure

Disclosure	FirstRand	Standard Bank	Absa Bank	Nedbank	Industrial & Commercial Bank of China	China Construction Bank	Bank of China	Agricultural Bank of China
Cyber term search	2	28	11	48	2	2	3	0

Results indicated that the South African reports yielded a higher level of disclosure based on a word search than the banks of China. The related words were found 89 times in the South African reports in contrast with only seven times referred to in the China reports.

Concerning the South African banks, Nedbank had a count of 48, ABSA had a count of 11, Standard Bank, 28 and First National Bank had only two. The China banks yielded a much lower count, with the Industrial and Commercial Bank of China showing two, the Bank of China having three, the Agricultural Bank of China having a count of two and the China Construction Bank not referencing any of the terms at all.

8. Conclusions

Both countries chosen for the study must comply with different reporting requirements. South Africa is subject to the JSE listing requirements, including IFRS and King IV (JSE, 2017). To produce an integrated report is one of the requirements as per King IV. King IV also requires organisations to provide reasons for not submitting integrated reports (IODSA, 2016).

China is subject to the CASC listing requirements, including IFRS and CBRC (CASC, 2018). In addition, cyber risk reporting is a legal requirement in specific South Africa and China (Ning & Wu, 2019; SEC, 2012). Both IFRS and King IV are required to disclose all risks (IFRS, 2018; IODSA, 2016).

As it is referred to by some banks in China, cyber risk, or information technology risk, forms part of their operational risk portfolio. Both South Africa and China have legislation and cyber risk reporting policies that fall outside the IFRS and King IV requirements. However, this legislation and policies, the POPIA and the Chinese Cybersecurity Law, are relatively new and thus not fully implemented (Ning & Wu, 2019; Sophos, 2019). This statement paralleled with the insufficient disclosure of China's banks. Furthermore, there is no specific framework for cyber risk reporting used by China's banks. However, their annual reports show that this is incorporated in their primary risk policy documentation.

A total of six governance-related questions, focusing on risk reporting, cyber risk reporting and policies, were utilised in building the disclosure index. It was found that all the banks in the sample have policies in place regarding risk reporting, but only three (all of the South African banks) specifically indicate that they have cyber risk policies in place. These results mean that only 38% of the total sample have a cyber risk policy.

Seven out of the eight banks state that they have strategies to manage cyber risk, which is 88% of the total sample. However, the banks' in China classifies cyber risk under their operational risk portfolio and refers

to risk management strategies in general. Only one bank, the Agricultural Bank of China, did not mention such a strategy. These results indicate that 100% of the South African banks have strategies to manage cyber risk, whereas only 75% of the Chinese banks have such strategies. Of the eight banks, only three South African banks identified cyber risk as a material item, 38% out of the total sample.

The banks chosen for this sample complied with 67% of the governance questions asked. However, when looking at the countries individually, China only had a 46% compliance rate, where South Africa had almost double that at 88% compliance. Only Absa and Nedbank had complied with all the questions. Only two banks provided risk rankings. That is 25% of the total sample size, all of which were South African banks. Absa ranked cyber risk as their number one risk, and Nedbank ranked cyber risk as their second most critical risk. The other 62% of the sample did not rank cyber risk.

The World Economic Forum (2015) stated that the financial impact within the first few days is estimated to be around $ 250 billion in the extreme event that internet connections worldwide go down. Furthermore, in a study done by Hovav & D'Arcy (2003), results show a negative share price effect for organisations, such as banks, that have a business model heavily reliant on the internet when they fall victim to cyber incidents. However, from all the banks sampled, no single cyber risk incident was disclosed for the 2018 financial year. This could be due to no cyber-attacks occurring during the 2018 financial year or that organisations are reluctant to disclose this information out of fear of possible attacks even though regulators require it.

Eling and Schnell (2016) state that to actively manage cyber risk, risk mitigation is a lot more plausible than risk avoidance. Risk mitigation, along with the support of various instruments (e.g., anti-virus and firewalls), has proven to be most effective in reducing the probability of occurrence and minimising the size of losses. Furthermore, 100% of the banks showed that they do have risk mitigation procedures in place.

9. Managerial Implications

When analysing the results from the study, it is concluded that the disclosure practices on cyber risks of the banks differ substantively between the two countries. These differences between countries have implications if potential investors or any stakeholders would like to make any comparisons.

Cybersecurity is a critical factor in banking operations because of digital technology advancements. The annual reports of China's banks classify risks under different categories. Cyber risk and information technology risk is classified as operational risks. As a result, China does not explicitly refer to cyber risk but only discloses it as an operational risk in its annual reports. No ranking is associated with any of their risks or categories. This is in contrast when compared to the South African annual reports as South African banks clearly define cyber risk and rank it amongst their top risks. They also recognise it as a material item.

From a South African reporting perspective, cybersecurity is one of the most significant risks in the banking sector. It is precisely defined and referred to in the annual reports. For stakeholders, it is easier to assess the impact of cybersecurity from a South African company as the information is more specific and available.

For the 2018 financial year, there were no reported cyber risk incidents in either country. For China, however, as per Chinese Cybersecurity Law, if any cyber-attack poses a risk to national security, such an incident will not be published. This could mean banks have been prohibited from reporting it to anyone, except the relevant authorities, if any incident occurred.

Based on this study, it is evident that South Africa's banks provide more defined and relevant cyber risk information. In conclusion, integrated reports published by South African banks are of a higher quality when compared to China's banks' annual reports.

To conclude, companies need reinforce their cybersecurity disclosures. This reinforcement and emphasis are needed to demonstrate accountability and to enhance stakeholder trust around cybersecurity.

Reference List

Al-Hadi, A., Hasan, M.M. & Habib, A. 2016. Risk committee, firm life cycle, and market risk disclosures. *Corporate Governance: An International Review*, 24(2):145-170.

Amran, A., Manaf Rosli Bin, A. & 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.

Asongu, S., Akpan, U.S. & Isihak, S.R. 2018. Determinants of foreign direct investment in fast-growing economies: evidence from the BRICS and MINT countries. *Financial Innovation*, 4(1).

Barry, T., Jona, J., & Soderstrom, N. (2022). The impact of country institutional factors on firm disclosure: Cybersecurity disclosures in Chinese cross-listed firms. *Journal of Accounting and Public Policy*, 106998.

Berry, C. 2018. Cyberattacks targeting South Africa: expensive lessons to be learnt. Available at: https://www.camargueum.co.za/post/cyberattacks-targeting-south-africa-expensive-lessons-to-be-learnt (accessed 11 November 2019).

BIS. 2013. Principles for effective risk data aggregation and risk reporting. Available at: https://www.bis.org/publ/bcbs239.pdf (accessed 3 June 2020).

Bouveret, A. 2018. Cyber risk for the financial sector: a framework for quantitative assessment: International Monetary Fund.

Bryman, A. & Bell, E. 2014. *Research methodology: business and management contexts*. Cape Town: Oxford University Press Southern Africa.

Businesstech. 2017. Battle of the banks: how S.A.'s big five banks compare. Available at: https://businesstech.co.za/news/banking/182873/battle-of-the-banks-how-sas-big-five-banks-compare/ (accessed 25 July 2018).

Businesstech. 2018. These are South Africa's biggest banks. Available at: https://businesstech.co.za/news/banking/245061/these-are-south-africas-biggest-banks/ (accessed 5 October 2019).

Businesstech. 2019. These are the ten biggest overall risks for South Africa. Available at: https://businesstech.co.za/news/business/337839/these-are-the-10-biggest-overall-risks-for-south-africa/ (accessed 10 November 2019).

Cantoria, C. 2019. Risk Mitigation Strategies and Risk Mitigation Plan: Tips for Documentation & Implementation in Project Management. Available at: https://www.brighthubpm.com/risk-management/47934-risk-mitigation-strategies-and-risk-mitigation-plan/) (accessed 10 November 2019).

Carels, C.M. 2014. Integrating reporting: an analysis of the extent of social environmental and ethical matters in corporate reporting.

CASC. 2018. China Accounting Standards Committee. Available at: http://www.casc.org.cn/2015/1123/123195.shtml (accessed 28 July 2018).

chinaplus.cri.cn. 2018. China holds top four rankings in list of the world's largest banks. Available at: http://en.ce.cn/Business/topnews/201807/05/t20180705_29633951.shtml (accessed 28 July 2018).

CIMA. 2008. Introduction to managing risk. Available at: https://www.cimaglobal.com/Documents/ImportedDocuments/cid_tg_intro_to_managing_rist.apr07.pdf (accessed 17 February 2020).

Cruickshank, C. 2019. Beware the evolving beast: cybersecurity in financial services. Available at: https://www.ocorian.com/article/beware-evolving-beast-cybersecurity-financial-services (accessed 11 September 2019).

Deloach. 2019. 10 Top Risks for 2019. Available at: https://www.corporatecomplianceinsights.com/10-top-risks-for-2019/ (accessed 2 October 2019).

Deloitte. 2012. Core beliefs and culture Chairman's survey findings. Available at: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-core-beliefs-and-culture.pdf (accessed 9 September 2019).

Demrovsky, C. 2019. Don't Ignore These 10 Global Business Risks In 2019. Available at: https://www.forbes.com/sites/chloedemrovsky/2019/01/14/dont-ignore-these-10-global-business-risks-in-2019/#3ecbaba914c0 (accessed 10 November 2019).

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, *13*(2), C1-C9.

Eling, M. & Schnell, W. 2016. What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(5): 474-491.

Eling, M. & Wirfs, J.H. 2016. Cyber Risk: Too Big to Insure?: Risk Transfer Options for a Mercurial Risk Class. Institute of Insurance Economics I. VW-HSG.

Elshandidy, T. & Neri, L. 2015. Corporate Governance, Risk Disclosure Practices, and Market Liquidity: Comparative Evidence from the U.K. and Italy *Corporate Governance: An International Review*, 23(4):331-356.

Elshandidy, T., Shrives, P.J., Bamber, M. & Abraham, S. 2018. Risk reporting: A review of the literature and implications for future research. *Journal of Accounting Literature*, 40:54-82.

Epstein, M.J. & Rejc, A. 2006. *The reporting of organisational risks for internal and external decision making*. CMA, Canada.

Fleming, S. 2019. The top 10 risks to the global economy, according to the Economist Intelligence Unit. Available at: https://www.weforum.org/agenda/2019/03/the-top-10-risks-to-the-global-economy-according-to-the-economists-intelligence-unit/ (accessed 10 November 2019).

FRC. 2017. Risk and viability reporting. Avialable at: https://integratedreporting.org/wp-content/uploads/2017/11/FRBRisk-and-Viability-Reporting.pdf (accessed 5 October 2019).

Gao, L., Calderon, T.G., & Tang, F. 2020. Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems, 38. https://doi.org/10.1016/j.accinf.2020.100468.*

GRI. 2018. About Sustainability Reporting. Available at: https://globalreporting.org/information/sustainability-reporting/Pages/default.aspx (accessed 30 September 2018).

GRI. 2019. About GRI. Available at: https://www.globalreporting.org/information/about-gri/Pages/default.aspx (accessed 25 April 2019).

Hackston, D. & Milne, M.J. 1996. Some determinants of social and environmental disclosures in New Zealand companies. *Accounting, auditing & accountability journal*. 9(1): 77-108

Härle, P., Havas, A., Kremer, A., Rona, D.H.S. 2016. *The future of bank risk management*. Available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-bank-risk-management# (accessed 26 January 2020).

Hovav, A. & D'Arcy, J. 2003. The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, 6(2):97-121.

IFRS. 2018. List of IFRS Standards. Available at: https://www.ifrs.org/issued-standards/list-of-standards/ (accessed 25 July 2018).

IIRC. 2018. Why? The need for change. Available at: http://integratedreporting.org/why-the-need-for-change/ (accessed 2 October 2018).

IODSA. 2010. *King Report on Governance for South Africa 2009; King Code of Governance Principles for South Africa 2009; Companies Act 71 of 2008*. Cape Town: Jutalaw.

IODSA. 2016. King IV Report. https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/684B68A7-B768-465C-8214-E3A007F15A5A/IoDSA_King_IV_Report_-_WebVersion.pdf

IRCSA. 2013. The International Integrated Reporting Framework..

JSE. 2017. JSE Limited Listings Requirements.

Khlif, H., Ahmed, K. & Souissi, M. 2017. Ownership structure and voluntary disclosure: A synthesis of empirical studies. *Australian Journal of Management*, 42(3):376-403.

Klemash, S W., Smith, J. C. & & Seets, C. 2020. What Companies are Disclosing About Cybersecurity Risk and Oversight. Available at: https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/ (accessed 7 June 2022).

Khlif, H. & Hussainey, K. 2016. The association between risk disclosure and firm.

KPMG. 2017. Overview of China's Cybersecurity Law.

Li, H., No, W.G. & Wang, T. 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, 30:40-55.

Linsley, P. & Shrives, P. 2000. Risk management and reporting risk in the U.K. *Journal of Risk*, 3:115-129.

Linsley, P.M. & Shrives, P.J. 2006. Risk reporting: A study of risk disclosures in the annual reports of U.K. companies. *The British Accounting Review*, 38(4):387-404.

Mazumder, M., & Sobhan, A. (2020). The spillover effect of the Bangladesh Bank cyber heist on banks' cyber risk disclosures in Bangladesh. *Journal of Operational Risk*, *15*(4).

Newman, C. & Belknap, P. 2019. SEC Cyber Briefing: Regulatory Expectations for 2019. Available at: https://corpgov.law.harvard.edu/2019/01/02/sec-cyber-briefing-regulatory-expectations-for-2019/ (accessed 17 July 2020).

Ning, S. & Wu, H. 2019. China: Cybersecurity 2020. Available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china (accessed 17 November 2019).

Norton. 2019a. What is a data breach? Available at: https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html (accessed 10 November 2019).

Norton. 2019b. What is a distributed denial of service attack (DDoS) and what can you do about them? Available at: https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html (accessed 10 November 2019).

Norton. 2019c. What is a man-in-the-middle attack? Available at: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html (accessed 10 November 2019).

Norton. 2019d. What is a Trojan? Is it a virus or is it malware? Available at: https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html (accessed 10 November 2019).

Norton. 2019e. What is mobile ransomware? Available at: https://us.norton.com/internetsecurity-mobile-what-is-mobile-ransomware.html (accessed 10 November 2019).

Norton. 2019f. What is phishing? Available at: https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html (accessed 10 November 2019).

Norton. 2019g. What is spear phishing? Available at: https://us.norton.com/internetsecurity-malware-what-spear-phishing.html (accessed 10 November 2019).

Oliveira, J., Rodrigues, L.L. & Craig, R. 2013. Company Risk-related Disclosures in a Code Law Country: A Synopsis. *Australasian Accounting, Business and Finance Journal*, 7(1):123-130.

Regan, J. 2019. What is Malware? How Malware Works & How to Remove It. Avaiable at: https://www.avg.com/en/signal/what-is-malware (accessed 10 November 2019).

SABRIC. 2019. Digital Banking Crime Statistics. Available at: https://www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics/ (accessed 11 November 2019).

SARB. 2012. Regulations Relating to Banks. *35950*.

SARB. 2019. Directiver 2/2019. 15/8/1/3.

SEC. 2012. Proxy Disclosure Enhancements. Available at: https://www.sec.gov/rules/final/2009/33-9089-secg.htm (accessed 10 November 2019).

Securities & Commission, E. 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. *February* 26:2018.

SEC, Statement on Cybersecurity Interpretive Guidance. (2018), available at https://www.sec.gov/news/public-statement/statement-clayton-2018-0221 [https://perma.cc/RQR8-L8XF]

SECPCCD, (2018). Guidance on Public Company Cybersecurity Disclosures. https://www.sec.gov/rules/interp/2018/3310459.pdf [https://perma.cc/PL5D-58ZP] [hereinafter SEC Cyber Guidance].

Skinner, C. P. (2019). Bank disclosures of cyber exposure. *Iowa L. Rev.*, *105*, 239.

Sophos. 2019. Only 34% of South African organisations ready to comply with the POPI Act. Available at: https://www.itweb.co.za/content/nWJadvb8z3bMbjO1 (accessed 11 November 2019).

Stubbs, W. & Higgins, C. 2018. Stakeholders' perspectives on the role of regulatory reform in integrated reporting. *Journal of Business Ethics*, 147(3):489-508.

Thun, T. 2015. European Banks Underestimate the Challenges of BCBS 239 Implementation.

Tylor, H. 2018. What Are Cyber Threats: How They Affect You and What to Do About Them. Available at: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/ (accessed 17 November 2019).

Wang, Z., Chen, J. & Zhao, X. 2018. Risk Information Disclosure and Bank Soundness: Does Regulation Matter? Evidence from China. *International Review of Finance*, n/a(n/a).

Warren, P., Kaivanto, K. & Prince, D. 2018. Could a cyber attack cause a systemic impact in the financial sector? *Bank of England Quarterly Bulletin*, 58(4):21-30.

Wilson, H. 2014. UBS banker banned over $2.3bn rogue trading scandal.