Invisible Ubiquity - Cloud Security in UK Corporate Annual Reporting

Bob Duncan*, Mark Whittington†
Business School
University of Aberdeen
Aberdeen, UK
Emails: *robert.duncan@abdn.ac.uk, †mark.whittington@abdn.ac.uk

***Abstract*—The cloud is embedded in the operations of large businesses, who will understand the incentives in terms of cost reduction but also need to recognise, accept and mitigate the risks that come with adoption of an approach that brings in more actors and more opportunities for rogue interventions. We address the extent to which the five quoted UK banks, as an interesting sample of UK quoted corporates, inform their shareholders of the benefits and risks of cloud use through the traditional official medium of the annual report. There has been a rise in pressure, whether legal, quasi-legal or perceived best practice, to report significant risks to the business and it would be reasonable to assume that using the cloud might be such a risk. A study of the banks' lengthy reports, with over 1,600 pages across the five reports for 2017, shows minimal mention of cloud as a risk, but the use of "cyber" as the term for, it seems, internet and computer risks of all kinds. The reports focus on directors overseeing and making themselves aware of risks with much of the language vague with key terms not defined. Standard Chartered, however, seems to take a different and, it is suggested, a more constructive approach than their peers.**

Keywords–FTSE100 companies; GDPR compliance; cloud forensic problem.

I. INTRODUCTION

Large corporates have always been interested in embracing outsourcing technologies [1], and in particular IT. With many decades of experience, they have become very good at it, and understand the risks well. They also understand the value of using the best of technology for their business and were quick to realise the added value that outsourcing gave them, allowing them to access better and faster technology, without having to invest inordinately high sums of money to achieve their objectives.

With cloud now into its second decade of evolution, it is no longer the novelty architectural solution to corporate IT problems, but has rather become an accepted part [2] of the process of doing business. The rapid scalability of cloud resources allows expanding resource requirements for even the largest of corporates to now be considered an everyday event. Indeed, it is so ubiquitous that you will be hard pressed to find any large corporate who does not enjoy its benefits in a multiplicity of ways today.

That does not mean the inherent security issues of cloud are now a thing of the past. Indeed, many of these risks remain to this day [3]. However, it is clear that with many decades of experience in outsourcing IT behind them, large corporates have developed a much deeper understanding of many of the risks involved, with more of a "can do" approach than many smaller companies seem to be able to manage.

Achieving information security with conventional distributed network computer systems continues to present a significant challenge, and cloud still continues to present difficulties towards achieving this end. The principal reason for the difficulty of this challenge remains the not yet fully resolved "Cloud Forensic Problem" [4]. This arises once an attacker gains a foothold in a cloud system and becomes an intruder. Once this happens, there is little to prevent the intruder from helping themselves to any amount of data, either by viewing, modifying, deleting or ex-filtrating it from the victim system. Worse still, there is nothing to prevent the intruder from gaining sufficient privileges to completely delete all trace of their attack. While there is still no bulletproof solution, where appropriate mitigatory steps are taken, the risk can be significantly reduced. It is clear that serious monitoring must take place continuously.

Large corporates also understand well the need to achieve legislative and regulatory compliance, as well as the potential penalties for failure to deliver such compliance. They do have the advantage of having adequate resources at their disposal, meaning they have no difficulty in accessing the best expertise to deal with any situation. They certainly are aware of both the financial and reputational consequences of compliance failure.

Thus they have a clear view of the incentives, both for compliance and the benefits to their business by ensuring that all the people they deal with are also in a position to achieve compliance. Knowing who you are dealing with and understanding that they too are compliant, ensures a far higher level of trust, which in turn ensures there are less likely to be issues surrounding compliance failures.

We start in Section II, by considering the cloud specific issues that present a barrier to good security and privacy with cloud use. In Section III, we consider IT and cloud risk reporting to shareholders in large corporates and in Section IV, we consider how this is approached by the 5 largest UK banks listed on the FTSE100 Index. In Section V, we look at the requirement UK banks have to report to shareholders. In Section VI, we discuss our findings, and in Section VII, we discuss our conclusion and make our recommendations.

II. CLOUD RISK AND SECURITY ISSUES

IT risk has become a more prominent feature of risk reporting in many jurisdictions, including the UK [5]. Over and above the other risk and security issues with IT, cloud adds

 ISBN: 978-1-61208-703-0

a further level of issues and of questions that need answers. There are a great many additional risk vectors which come into play once cloud computing is deployed. It is not just a case of getting past the corporate firewall and through the internal defence network of the organisation, but in addition, attackers do not even have to get inside corporate systems. They can attack network traffic to and from the cloud instances. They can attack the Cloud Service Provider (CSP) direct, or through side channel attacks from their own, or other compromised systems. They can attack third party service providers, they can attack through compromised Internet of Things (IoT) networks, which are notoriously insecure.

Cloud systems are generally multi tenanted, with a range of other users. Proper partitioning between different clients can present non trivial challenges within the cloud environment. Achieving and maintaining proper access controls is another challenging area. Cloud systems can be vulnerable to Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks. Achieving and maintaining proper configuration of client based systems to use the cloud from within the corporate network systems can also present a huge challenge.

Why would large corporates want to use outsourced resources for their IT? What is the incentive for large corporates to use cloud? All major cloud service providers make much of the benefits of using cloud for businesses. We believe the following would be the most appropriate incentives for large corporates to use cloud:

- Access Anywhere, Anytime;
- Cost-Effectiveness;
- High Scalability;
- Improved Disaster Recovery;
- Improved Uptime;
- Multiple Migration Options;
- Sophisticated Security.

What kind of cloud deployments would they be interested in? Here are some examples of the most appropriate cloud deployments for use in large corporates:

- Accounting systems;
- Business to Business (B2B) systems;
- Corporate eMail systems;
- Corporate forecasting tools;
- Customer Relationship Management (CRM) systems;
- Enterprise Resource Planning (ERP) systems;
- Human Resources (HR) systems;
- Online web systems for both information and trading;
- Supply Chain Management (SCM) systems.

What kind of issues would they be likely to face in using cloud for these cloud deployments? Here are some examples of the kind of challenging issues they might face:

- Abuse of Cloud Systems;
- Account or Service Traffic Hijacking;
- Data Breaches;
- Data Loss;
- Denial of Service;
- Insecure APIs;
- Insufficient Due Diligence;
- Malicious Insider;
- Malware Injection;
- Shared Vulnerabilities.

Why would these present a particular challenge? The primary security goal of all companies is to achieve Confidentiality, Integrity and Availability (CIA) of their data. For cloud use, the CIA objective must still be met. We will briefly look at each of these issues in turn:

A. Abuse of Cloud Systems

Attacking encrypted systems, for example, is a difficult task to complete computationally. Some attackers will abuse cloud systems by gathering significant cloud resources to carry out malicious attacks on others. This is not easy to detect, unless particular attention is paid to high volume activity through log analysis.

B. Account or Service Traffic Hijacking

If account details are stolen, often through phishing, vishing, social engineering, and other non-technical attacks, as well as through technical means, including cross site scripting and traffic attacks, this can give an attacker a solid base from which to attack the overall system. It also allows the attacker a base from which to gain access to other systems more easily, as well as an opportunity to insert malware into the system.

C. Data Breaches

A data breach is the result of an intrusion which is most likely to be both malicious and intrusive. Because of the communication speed of cloud resources, any breach can result in mass data becoming exposed. This means data breaches are a particularly worrying attack, which can have devastating legislative and regulatory compliance consequences.

D. Data Loss

Data loss can arise for a number of different reasons. The data owner could lose the encryption key rendering the data useless. An authorised user might delete data accidentally. An intruder might maliciously delete data. There could be a physical failure of storage media, which if not properly backed up could result in data loss. Where proper backups are not in place, all these examples have the same result — the data is irretrievably lost.

E. Denial of Service

This is an old attack which attempts to disrupt business by flooding the system with hundreds, thousands or millions of automated requests for service. If not detected and dealt with, this brings the system to a halt, effectively closing down the availability of the system. It is like being caught in a rush hour traffic jam — you can neither go forward to your destination, not backwards to try to find an alternative route through, meaning you have to sit there doing nothing until the traffic clears.

F. Insecure APIs

Cloud computing brings with it the dichotomy of trying to make services available to millions yet keep systems secure at the same time — two incompatible goals. That solution has been the public facing Application Programming Interface (API). OAuth, and open authorisation service for web services which control third party access has been developed to help with this task.

 ISBN: 978-1-61208-703-0

G. Insufficient Due Diligence

Many companies fail to perform adequate due diligence to understand the full implications of using cloud before they embark on using cloud. Often companies expect well protected internal systems to work really well when they push them to cloud and fail to grasp the subtle differences between the two environments, leading to introducing weaknesses to their system.

H. Malicious Insider

Where a company depends solely on the cloud service provider for their security — they are at increased risk of exposure to malicious user attacks. This is especially problematic where the encryption keys are kept in the cloud, rather than securely in the company's own internal systems. Consider the damage caused by the Edward Snowden leaks.

I. Malware Injection

Malware injections are scripts or code embedded into cloud services, which then purport to provide valid SaaS instance services to cloud servers. This allows the code to perform malicious actions to eavesdrop on company traffic, compromise the integrity of sensitive areas, exfiltrate sensitive data, or perform any number of malicious actions on behalf of the attacker to the detriment of the company.

J. Shared Vulnerabilities

Cloud security is a function that must necessarily be shared between provider and client. Each party has the responsibility to take appropriate action to safeguard and protect the data. This means the provider must provide a secure environment in which to operate, but equally, the user must take responsibility for ensuring that they take proper precautions to secure user passwords and access restrictions to both data and devices, preferably by the use of multi-factor authentication.

III. IT and Cloud Risk Reporting to Shareholders in the UK

Quoted UK companies have a significant responsibility to report on their performance and, increasingly, their risks to their shareholders as well as other stakeholders. This responsibility is partly legally defined and necessary and partly voluntary. Some content falls between these two neat categories as the law might dictate a heading to be covered and then the approach and the level of detail to adequately address this is determined by the company with the oversight of their auditor. Risk is an area in this mezzanine category with paragraph 414c of The Companies Act 2006 (Strategic report and Directors' Report) Regulations 2013, No 1970 [6] stating that the strategic report for the company, which is the main descriptive part of the annual report, must contain "(a) a fair review of the company's business and (b) a description of the principal risks and uncertainties facing the company". This legislation reflects a growing trend towards the encouragement of more non-financial reporting such as the EU non-financial disclosure directive (2014) [7].

Companies, of course, face many risks of which cloud is only one. As we have seen, however, it is becoming a risk concerning not just known, narrowly defined problems but a more pervasive background to the entirety of "doing business". In this context, it is interesting to address the question of how much companies feel they need to tell their shareholders concerning their reliance on the cloud and the risks their business consequentially has embedded in it.

IV. Introduction to Banks

In order to focus our investigations into this question, we will consider the five banks quoted in the FTSE100 index as at October, 2018. These were Barclays, HSBC, Lloyds, RBS and Standard Chartered. Banks, perhaps more than any other industry, have layer upon layer of required reporting — some nationally determined, some internationally — some general, some very bank specific. Banks are a particularly interesting sector as, it is often argued, the rest of the economic system is dependent on the survival of the systemic or "too big to fail" members of the sector. It could be argued that in seeking to address the problems highlighted by the 2008 financial crisis, banks have been more regulated than they have been reduced to sizes that might solve the too big to fail issue. Hence, now banks report to, and are monitored by, their "host" government and by global banking supervisory bodies, for example the Financial Stability Board, as well as their traditional owners and masters — their shareholders. On top of this other stakeholders (customers, creditors, employees, etc.) are increasingly recognised by corporate governance codes, as the Financial Times [8] puts it "When only shareholders matter, there is only one constituency to disappoint. As capitalism tilts slowly to recognise other shareholders, General Motors is showing the way in how to let multiple interested parties down." So, for this sector in particular, there are many concerned overseers and it will be interesting to see what general or narrow cloud risk gets through the filter to reach the owners (aka shareholders).

Banks have often been in the eye of the news websites for disappointing IT related performance and, in a business model that relies more on web-enabled software than traditional branches or face-to-face contact, they are a key focus of the dependability and trustworthiness of IT systems remembering that disappointed customers may well take actions that will lead to disappointed shareholders. Whilst the engagement with cloud is often implicit and assumed rather than stated, there is no doubt that cloud is critical and will be become more so as the banks seek to increase efficiency by becoming more virtual and less physically accessible. This shift inevitably changes the risk profile of the banks and, while potentially reducing some risks (physical stealing of actual notes, for example), it will mean a raised level for online risks that any organization might struggle to keep up with.

V. Banks' Requirement to Report to Shareholders

There is a logic to risk reporting being less clearly defined than, say, the reporting of financial statements. Whilst all companies have sales and costs, the types and level of threat posed by differing risks will vary considerably by industry, as would the importance of various environmental issues between a bank and an oil company. There is a developing literature focused on risk reporting (see [9] for a literature review) and a concern that the idea of risk itself is not clearly conceptualised [9](pp 54). Whilst directors have a requirement to report issues of material and strategic importance or threat to the company, it is clear that they would also wish to give the impression that they are indeed "managing" the company and that risks

 ISBN: 978-1-61208-703-0

are under control and mitigated. Banking, in particular, has developed a multi-dimensional set of risk frameworks for bank-specific risks (credit risk, liquidity risk, market risk — see the annual reports of our case companies for more details) and, perhaps this leaves little room for the more mundane "normal risks" that face other businesses from their operations and systems. Nevertheless, it would seem that a cursory glance at the popular press and IT industry news feeds would suggest there might be much to make sure shareholders are aware of.

The methodology used here is that of content analysis an approach that seeks to examine qualitative information by turning it into quantitative data. This approach can address many questions the tone and style of reports, the relative importance through comparing quantities of mentions on differing topics, highlighting which topics merit graphs or pictures as opposed to just words, would be just three of many angles one might take. Such studies have looked at environmental, social, governance, risk and other areas of corporate reporting. The issue of confusing the measurable "quantity" with the less definable "quality" presents many issues and problems. Repeated mentions of the same information may show some recognition of importance, but does not impart more knowledge. One truth is that whilst "quantity does not mean quality", "no quantity means no quality". We find, perhaps surprisingly few (and oft repeated) direct mentions of "cloud" or even the broader "cyber" within the long five reports we examine. Hence our approach is adapted to become more discursive and less numerically focused as we seek to modify our methods to fit the data that presents itself. This highlights a further issue in studies such as this; that statistical sophistication, whilst desirable, is only possible when there is plenty of data, yet there are many topics that might be even more important but without the data quantities to satisfy the number-crunching desires of top academics.

VI. Cloud in the Banks' Annual Report

Banks do not only report using their "Annual Report". Like any other large, listed company there will be interim or quarterly reports along with a regularly updated website. Producing a "Corporate Citizenship" report, however titled, is usual and, if there is a share quote on a USA exchange, then a US reporting format referred to as a 20-F. Specific banking rules also require a Pillar 3 report covering their approach to having adequate capital. Focusing on the Annual report, banks have much to include, yet there is no word or page limit. Table I below shows the pages in each of the latest (October, 2018) annual reports for the 5 banks and the number of pages specifically in the risk section — of course, risk will probably also appear elsewhere in the report.

TABLE I: BANK PAGE STATS 2017 ©2019 Duncan and Whittington

Bank	AR Date	Length (pages) AR pp	Risk pp	% Risk
Barclays Bank	31/12/2017	328	87	27%
HSBC Holdings	31/12/2017	274	57	21%
Lloyds Banking Group	31/12/2017	278	50	18%
Royal Bank of Scotland Group	31/12/2017	419	80	19%
Standard Chartered	31/12/2017	344	74	22%

In a review of risk reporting in another UK industry (food producers), Abraham and Shrives [10] found a majority of general rather than specific disclosures and that content was repetitive over time They took this to imply that the companies were showing a concern to disclosure (symbolic) rather than offering substantive content. Such an approach may be more difficult for companies to achieve in 2017/2018 as audit coverage is somewhat broader than in the years 2002-2007 used in their survey and now includes the auditor having a check of much of the discursive section of the report. As stated above, there are many categories of risk that banks are required to take account of before they might turn to consider areas where reporting might be more voluntary and would have similarities with non-financial businesses. These are usually referred to as "operational risk" disclosures. Only one paper has considered banking operational risk disclosures in Europe [11] and this makes no specific reference to cloud, IT or internet risk issues. A critical flaw in the use of content analysis is that there needs to be some relevant content that is available for analysis and, hence, perhaps, the approach taken did not focus on such details.

Reviewing the five lengthy reports reveals some differing approaches. Whilst all five are "banks", they are not the same and do not face the same risks. Lloyds is a UK-focused retail bank whilst the other four include the wide breadth of investment banking too. RBS is still recovering from the financial crisis and continuing government ownership of a majority stake. Different activities will lead to different risks and therefore direct comparison may not be meaningful. Also, there is significant repetition in some of the reports which, a common issue with content analysis, can lead to statistics which show a great deal of disclosure when there is actually one disclosure ten times. Hence, a more discursive rather than numerical approach has been adopted.

"Cloud" rarely appears in any of the reports and not in a risk context. HSBC and Standard Chartered do not mention cloud once in their reports. Barclays launched a customer product called "Cloudit" and, more usefully, Lloyds states: "To support our transformation and deliver further efficiency savings, we will simplify and modernise our IT architecture while deploying new technologies such as cloud computing to enhance our capabilities and increase resilience." (Page 16, Lloyds — Digitising the group — Leveraging new technologies) This is confirmation of our expectation of "cloud behind the scenes". RBS, in a similar vein, states: "Faster repositioning of the bank's existing distribution network and technology platforms towards mobile, cloud based platforms and virtualisation." (Page 13, RBS)

"Cyber", on the other hand, either by itself or as the initial part of a word or phrase (cybersecurity, cyber-attack, cybercrime, etc.) is used to cover most information systems, internet and distributed computing concerns and solutions. The RBS quote below shows such an example: "Delivering appropriate digital infrastructure is important to ensure a 'technically-able' bank that supports its long-term future. Cyber security is also a vital part of providing a safe and secure banking service. Banks need to proactively identify and manage risks and efciencies in their operations and facilities" (Page 39, RBS)

The tables below (Tables II, III, IV, V and VI) show some of the key content in each of the reports — there seems a focus on showing that the directors have cyber covered in their board and risk committee structures. Interestingly, some banks have cyber risk mostly within operating risk, whereas Lloyds

and, more prominently, Standard Chartered now have it as a primary risk category on its own. Two banks had directors who might be seen to be experts in this field, a third had developed a system of named specialist external advisors to make sure there was such expertise. Three banks mentioned cyber within bonus objectives for one or more of the directors. Heavy investment in resilience and technology was mentioned frequently but without financial numbers. The audit row of the table shows the variety of length of the audit reports and also that there appears to be a bespoke approach with different cyber risks being highlighted by the audit firm, or, indeed, with HSBC, none at all. Despite the number of data breaches suffered by banks in previous years, the GDPR (General Data Protection Regulations) makes few explicit appearances in these reports, even though implementation was only a few months away when the reports were written. Only Lloyds has more than two mentions within their lengthy reports, with Barclays the only one to highlight the size of potential fines.

TABLE II: BARCLAYS BANK 2017 [12]

Item	Description
Key Point	New Centre of excellence for cyber security as part of restructuring
Comments in introductory pages	Investing in digital and mobile capabilities with an awareness of the cyber risk management
Risks highlighted	Cyber crime as a risk to the bank's business model. Model is stress tested with cyber attacks) Increased compliance costs as regulators focus on cyber risk
Directors	CEO has a target of strengthening cyber readiness
Committees	Risk committee sees the cyber theme as part of operational risk Cyber has reputational risk
Audit KPMG 6pp	User access management. Some concerns about developers, but found no reason to investigate further

TABLE III: HSBC HOLDINGS 2017 [13]

Item	Description
Key Point	"dominant threat"
Comments in introductory	rising cyber threat risk
Risks highlighted	Cyber threat Unauthorised systems access
Directors	Non-exec director is a security expert CEO has a cyber personal objective
Committees	Also a Financial Systems Vulnerability Committee
Audit PWC 5pp	No comments

TABLE IV: LLOYDS BANKING GROUP 2017 [14]

Item	Description
Key Point	" near term challenges new threats from data and cyber security" (P2)
Comments in introductory pages	"UK's largest digital bank" (P9) Information and cyber security policy are also included as part of the Human Rights commitment
Risks highlighted	IT infrastructre, cyber risk, 3rd party reliance Operational risk has cyber as a secondary section. List of potential cyber damage on page 135
Directors	Chief Operating Officer is assessed on mitigating evolving risks, including cyber
Committees	Board risk committee report separates out "IT and cyber risk" from operational risks
Audit PWC 8pp	Highlights access concerns, but additional testing found this to be secure

Uniquely, at least in this small data set, RBS provide a section of "additional information" from page 357 which extends for 50 pages which includes further risk factors. Whilst

TABLE V: ROYAL BANK OF SCOTLAND GROUP 2017 [15]

Item	Description
Key Point	"a key operational competence"
Comments in introductory	Refers to a multi-layered defence to cyber security , systems enhancements and training
Risks highlighted	Financial malware
Directors	No comment
Committees	Risk Committee receives bi-annual Resilience and Security report where cyber is highlighted Simulated cyber attack scenarios undertaken
Audit EY 14pp	Review of IT systems and controls mentioned, but no concerns found

TABLE VI: STANDARD CHARTERED 2017 [16]

Item	Description
Key Point	Not complacent. Further enhancing cyber security (P6)
Comments in introductory	We have made significant progress in our work to combat financial crime and have increased focus on our cyber risk management capabilities (p33) Mentions cyber security industry working bodies that it sits on
Risks highlighted	Information and cyber security raised to principal risk level
Directors	Directors joined by specialist external advisor on risk committee and subcommittee
Committees	Board Financial Crime Risk Committee Committees on Cyber Security and Cyber Threat Management mentioned
Audit KPMG 8pp	IT risk highlighted with discussion of controls and access - in relation to financial reporting found acceptable

one cannot be entirely sure, this approach may well put this section beyond the reviewing eye of the external audit team. We will focus on the aspects of Standard Chartered's reporting that would appear to differentiate it from the other banks. The additional information includes more detail on dependency on IT systems, reputational damage of loss of customer data, potential for fines, cost-saving focus undermining resourcing improved security amongst others. On page 389, a cyber act as part of a geopolitical event is mentioned as a further potential problem.

Apart from this RBS appendix, Standard Chartered would seem to have the most thorough and structured discussion of cyber risk. It stands out by giving a definition of information and cyber security risk as: "the potential for loss from a breach of confidentiality, integrity or availability of the Group's information systems and assets through cyber attack, insider activity, error or control failure" (page 162, Standard Chartered). It would seem the other banks take for granted the assumption that the reader's understanding of cyber security risk as matching their own.

Standard Chartered also uniquely further describes its management approach to the risk: "The Group seeks to avoid risk and uncertainty for our critical information assets and systems and has a low appetite for material incidents affecting these or the wider operations and reputation of the bank" (page 34, Standard Chartered)

And finally gives an overview of its "risk appetite" for cyber security: "The Group seeks to avoid risk and uncertainty for our critical information assets and systems and has a low appetite for material incidents affecting these or the wider operations and reputation of the Group" (page 177, Standard

Chartered)

Page 177 explains Standard Chartered's approach to cyber risk including roles, committee structure and monitoring in a more accessible way, as well as defining terms when other banks just use words and spread any content throughout the report.

There is, of course, much that of necessity needs to be left out of an annual report. However, it is easy enough for a vigilant analyst or shareholder to find the evidence presented earlier in the paper from a variety of sources and form their own view of the banks' ability to get to grips with "cyber". The task of the annual report perhaps, would seem to be to present a calm assurance that all is under control or at least controllable. As the audit reports do not directly address the broader cyber risks, it is for the shareholder to decide whether presentation truly matches the reality they gather from elsewhere.

VII. Conclusion

We can see from Section II, that there are a great many possible additional threats to achieving proper security once cloud is introduced to the provisioning of IT resources for large corporates. Many of these are not trivial to resolve. Increased vigilance becomes one of the most important elements of any defensive plan, without which the business will be exposed to further risk.

In an industry with so many risks and where other risks are heavily regulated and require extensive coverage and reporting, it might seem unreasonable to expect depth and detail on cyber security. However, it is rising in prominence as a risk category and is mentioned as a threat to the integrity of the business model on at least two occasions. However superficial coverage of ill-defined terms appears the norm.

The comments and statements in these annual reports do not give great insight or detail, some of the banks appear to be emphasising a big picture that they are doing whatever they can to not only recognise but also match the cyber challenges that they face. There is only the briefest glimpse into what this means below the surface, apart from page 177 in Standard Chartered's report. Standard Chartered might be held up as a role model in the clarity of their reporting such response to peer pressure is a recognized feature of the analysis of corporate reporting. The recognition that terms need to be explained, especially when the term "cyber" seems so frequent and vague, and the attempt to bring together the information on the topic rather than spreading it through the report gives the impression of seeking to inform the reader rather than just ticking boxes in a structure designed to report on committees rather than subjects. Whilst impression management is another key theme within discursive reporting research, this awareness in itself is to be credited.

The annual report is the authorised vehicle for informing shareholders specifically about the success and risks of the business they own. The banks tend to focus on banking risk categories, and this might squeeze the word count available for more usual business risks. Banks, due to their size and importance, as well as their reliance on IT, including cloud, could do more to inform their owners about more than the committee structures and broad themes. Perhaps this traditional report structure is not the best way of doing this, yet Standard Chartered seem to have provided a higher degree of clarity and sharpness by defining terms and focusing a little more on topic than corporate structure.

References

[1] R. Babin, S. Briggs, and B. Nicholson, "Corporate Social Responsibility and Global IT Outsourcing," Commun. ACM, vol. 54, 2011, p. 28.

[2] J. Gubbi, R. Buyya, and S. Marusic, "1207.0203," Futur. Gener. Comput. Syst., vol. 29, no. 1, 2013, pp. 1–19.

[3] B. Duncan and Y. Zhao, "Risk Management for Cloud Compliance with the EU General Data Protection Regulation," in 7th Int. Work. Secur. Priv. Perform. Cloud Comput. (SPCLOUD 2018), Orleans, France, 2018, p. 8.

[4] B. Duncan, M. Whittington, and V. Chang, "Enterprise security and privacy: Why adding IoT and big data makes it so much more difficult," in Proc. 2017 Int. Conf. Eng. Technol. ICET 2017, vol. 2018-Janua, 2018.

[5] B. Duncan, Y. Zhao, and M. Whittington, "Corporate Governance, Risk Appetite and Cloud Security Risk: A Little Known Paradox. How Do We Square the Circle?" in Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization, Athens, 2017, pp. 1–6.

[6] U. Gov, "The Companies Act 2006 (Strategic report and Directors' Report) Regulations 2013," 2013. [Online]. Available: https://www.legislation.gov.uk/ukdsi/2013/9780111540169/part/2 Accessed: 28/03/2019

[7] EU, "(2) EU (2014) Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups." 2014.

[8] FT, "General Motors: Cruzing for a bruising," 2019.

[9] T. Elshandidy, P. J. Shrives, M. Bamber, and S. Abraham, "Risk reporting: A review of the literature and implications for future research," J. Account. Lit., vol. 40, 2018, pp. 54–82.

[10] S. Abraham and P. J. Shrives, "Improving the relevance of risk factor disclosure in corporate annual reports," Br. Account. Rev., vol. 46, no. 1, 2014, pp. 91–107.

[11] A. Barakat and K. Hussainey, "Bank governance, regulation, supervision, and risk reporting: Evidence from operational risk disclosures in European banks," Int. Rev. Financ. Anal., vol. 30, 2013, pp. 254–273.

[12] B. Bank, "Barclays Bank 2017 Annual Reort," Tech. Rep., 2017. [Online]. Available: https://home.barclays/investor-relations/reports-and-events/annual-reports/2017/{\%}0A Accessed: 28/03/2019

[13] HSBC, "HSBC Holdings 2017 Annual Report," Tech. Rep., 2017. [Online]. Available: https://www.hsbc.com/-/files/hsbc/investors/hsbc-results/2017/annual/hsbc-holdings-plc/180220-annual-report-and-accounts-2017.pdf Accessed: 28/03/2019

[14] Lloyds, "Lloyds Bank 2017 Annual Report," Tech. Rep., 2017. [Online]. Available: https://www.lloyds.com/investor-relations/financial-performance/financial-results/annual-report-2017 Accessed: 28/03/2019

[15] RBS, "Royal Bank of Scotland Group 2017 Annual Report," Tech. Rep., 2017. [Online]. Available: https://investors.rbs.com/{~}/media/Files/R/RBS-IR/annual-report-2017/royal-bankof-scotland-annual-report-and-accounts2017.pdf Accessed: 28/03/2019

[16] S. Chartered, "Standard Chartered 2017 Annual Report," Tech. Rep., 2017. [Online]. Available: https://www.sc.com/annual-report/2017/ Accessed: 28/03/2019

 ISBN: 978-1-61208-703-0