Corporate Governance, Risk Appetite and Cloud Security Risk: A Little Known Paradox. How Do We Square the Circle?

Bob Duncan
Computing Science
University of Aberdeen
Email: bobduncan@abdn.ac.uk

Yuan Zhao
Accounting and Finance
University of Aberdeen
Email: y.zhao@abdn.ac.uk

Mark Whittington
Business School
University of Aberdeen
Email: mark.whittington@abdn.ac.uk

***Abstract*—In today's corporate world, the notion of corporate governance has taken a more important role in the management of large corporates. There is a growing consensus that large corporates ought to take more of a stewardship approach to running a company in a clear attempt to move away from the agency theory approach, with all its attendant problems and issues. A fundamental component of corporate governance concerns the adequate recognition of risk faced by the organisation and dealing with it appropriately. Traditional corporate IT risk is well understood, as are the mitigation strategies needed to address this important area. Large corporates also understand risk theory well, and how finding the right balance between risk and profitability is key to ensuring profitability can be maximised while ensuring long term sustainability and resilience are also achieved. We assert that the cloud computing paradigm, while economically attractive to corporates, provides such a step change from traditional IT paradigms, that new risks have evolved, which are not well understood, leading to the possibility of unintended exposure to these sometimes considerable risks. We propose a different approach to the quantification of these risks, which we believe will provide a more robust approach to understanding the potential exposure they face when using cloud.**

***Index Terms*—Corporate governance; corporate stewardship; risk appetite; cloud security risk.**

I. Introduction

Achieving effective information security in the cloud is not a trivial process. There are many challenges to overcome, and sometimes those challenges arise from the most unexpected places. There are a great many influences, which bear down on the successful outcome of meeting this important goal, and often, a number of these influencing factors are not aligned.

This presents managers with something of a paradox when it comes to satisfying all the demands placed upon them, particularly when it comes to satisfying the rules of good corporate governance, managing risk effectively and balancing this with the primary goal of a company, which is to maximise the resources of that company for the benefit of the shareholders. This fiduciary responsibility of management to the shareholders has been a fundamental tenet of good corporate management for a very long time.

However, there is also a recognition that a company needs to be managed responsibly in a sustainable way to ensure the continued existence of the company, such that it be capable of withstanding sudden market shock, in other words is resilient to market forces, and added to this is the requirement to act in a responsible, accountable and ethical manner.

A modern requirement of a company is that there is now a recognition that information forms a key element of the resources of that company, and that it is therefore necessary to safeguard this information properly. This is further reinforced following the introduction of, sometimes punitive legislation [1][2], to ensure that companies achieve this goal.

For those member states of the EU, and for the UK post Brexit, there is a new "Bogey man" on the horizon — the forthcoming General Data Protection Regulation, which is scheduled to be brought into law in May 2018. This will require a considerable number of changes to be implemented in corporate systems in order to comply with this legislation. The level of fines proposed takes compliance fines to a new high, and will definitely attract the attention of board members.

In Section II, we discuss some background on all these issues. In Section III, we consider how the Financial Services Sector approach cyber risk, in Section IV, we consider why this might be important for company cloud users. In Section VI, we consider how this might work; and in Section VII, we discuss our conclusions.

In the next section, we will take a look at these important areas to see what we can learn.

II. Background

We start by looking at Corporate Governance, followed by Risk Appetite, IT Risk and Cloud Security. This first area we look at will be Corporate Governance.

A. Corporate Governance Literature

We can trace some of these issues back to the early 1930s, when Berle and Means [3], commented how setting up a large company was now beyond the means of any single person, which would lead to the popularity of the large company, where we would see the concept of the separation

of management and ownership. This, in turn, would ultimately lead to the evolution of Agency Theory [4]. One of the fundamental flaws of Agency Theory is the inability to control greed, and this became one of the fundamental weaknesses of this theory, leading to the uncontrolled growth of management remuneration.

In the UK, the financial de-regulation, which took place in the 1980s, would lead to extremes of corporate financial excess, including corporate scandals, such as the Bank of Credit and Commerce International (BCCI), Maxwell and the controversy over directors' pay. Government responded to this by commissioning the 1992 Cadbury Report [5]. This resulted in the introduction of the "Combined Code", to which all large UK corporates should adhere, by reporting in their annual return whether they "comply or explain" with the recommendations of the report. A year later, Jensen [6], wrote about the effect of technological innovation and internal control systems failures. Jensen and Chew [7] investigate the effects of the takeover boom of the 1980s. The Combined Code was subsequently updated [8]–[11].

Still in the UK, UK corporate governance continues to evolve with incremental but increasing awareness of corporate responsibilities to more than just shareholders and also a widening recognition of risk and societal impact — all relevant to cloud security. One recent example of this wider trend would be the Modern Slavery Act (2015) requiring an annual statement with a home page link explaining the steps the company has taken to expose and take out slavery in their supply chain [12]. This has some relevance as minor web breaches probably are not consequential to shareholders especially if not disclosed, in a similar way slavery is probably even advantageous — perhaps we are slowly moving away from shareholder dominance.

In the US, after the introduction of the Sarbanes-Oxley Act (SOX) in 2002 [1], Bauer et al [13], Bratton [14], Brickey [15], Holmstrom [16], Mitchell [17] and Rosen [18] all wrote about the implications for corporate governance. In the UK, Higgs [19], updated the Combined Code, and the effects of SOX were also addressed for the Financial Reporting Council [20]. The Organisation for Economic Co-operation and Development (OECD) [21] published its principles of corporate governance. Further updates to the code took place [22]–[25], and the next significant change occurred in 2012, when the Financial Reporting Council (FRC) recommended a new Stewardship Code be adopted [26].

It is worth pointing out that there is a fundamental difference between the approach adopted by the UK and the US. The UK have adopted a principles based approach, whereby general principles are established, and companies are required to "comply or explain" in their annual report. This means there is little need to constantly change legislation to keep up. By contrast, the US have adopted a rules based regime, whereby very specific legislation is enacted to determine what corporates must do. While the goals and requirements are generally clear, it has spawned a high-end legal and accounting industry, which constantly seeks to probe and push the boundaries in order to gain advantage, while retaining the ability to achieve compliance. Thus, the US government must constantly rewrite and update the rules to keep pace with these continuous attempts to subvert the rules — a considerable ongoing task. Regulators too, will have a more challenging task to keep on top of all these attempts to subvert the rules. Duncan and Whittington [27] provide some useful background on this area, including corporate legislation and standards compliance issues.

The clear and evolving message to come through from all these changes is that there is now a much greater emphasis on the need to identify and address risk properly. The global financial crash of 2008 really brought home the importance of effective risk management. Banks, in particular, had been "going through the motions" rather than really paying attention to the possibility that some of these risks were very real, and the consequences of failing to address them properly would have a catastrophic impact on not just their own business, but the global economy as a whole. It is also the case that financial regulators were themselves pretty much caught asleep on the job. Thus, we will next look at risk appetite.

B. Risk Appetite

Risk appetite can be described as the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives. Risk needs first to be properly identified, and the consequent financial implications properly measured or estimated should the risk identified arise. The probability of occurrence of each risk identified, must also be calculated. Such identified risks must then either be accepted, mitigated against, or declined, depending on the risk appetite of management. Usually, there is a correlation between risk and reward. The more profit that can be generated, usually the greater the risk the organisation is exposed to. Often, this risk considerably exceeds the potential amount of profit to be generated.

All companies generally have developed a mission statement, or vision statement. Where financial goals or targets are identified, it will be necessary to identify the risk requiring to be taken to achieve such goals and targets. This identifies the minimum required risk that must be taken in order to meet the goals or targets. If the risk required is unrealistic, i.e., too high, then the goals or targets should be adjusted, otherwise this will automatically lead the company to accept dangerous levels of risk.

In any event, the risk capacity of the company must be identified, as must the risk tolerance. These are not the same thing. Risk capacity tries to identify the extent to which the investment strategy can withstand negative events without seriously affecting the achievement of the goals or targets of the company. Whereas risk tolerance considers the extent to which a company is willing to risk a less favourable outcome in pursuit of a possible greater outcome. This can be considered a psychological trait, and if company managers happen to have have a high tendency towards the psychopathic spectrum of behaviour, there is a greater chance of a mismatch

arising between risk capacity and risk tolerance, leading to a less well considered attitude towards the real risk being undertaken [28].

This leads management to seek an economic equilibrium between profit and risk, such that they can maximise profit constrained by their understanding of risk. Where the company is run by prudent management, they will usually decide to accept those risks, which they understand really well, mitigate risks, which they are prepared to accept, but where they mitigate the extent of the risk accepted, possibly by the use of insurance, to minimise their exposure, and decline all risk they do not understand. This will usually lead to a safe performance, if somewhat unexciting. Duncan and Whittington [29], argued that where the management approach to running the company is biased towards the traditional agency based management approach, rather than a stewardship approach, the company is likely to have a higher risk appetite. Successful use of this high risk approach can lead to complacency over time, resulting in a more cavalier assessment of risk within the company, which can ultimately lead to hubris developing, leading to the acceptance of much higher risk levels than have been understood. When this approach goes wrong, the results can be catastrophic [30].

Risk culture in a company evolves from a system of values and behaviours present in that company, which will shape the risk decisions of management and employees. An important element of risk culture is the development of a common understanding of a company and its business purpose or aims.

C. IT Risk

In large corporates, the area of IT risk in traditional distributed systems is generally very well understood. There are some very good security standards, such as the joint International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (ISO/IEC), ISO/IEC 27000 [31], Control Objectives for Information and Related Technologies (COBIT) [32], and the Payment Card Industry Data Security Standard (PCI DSS) [33], which are well adopted by large corporates. Indeed, by 2012 [34], some two thirds of FTSE100 companies were either fully or partially compliant with the ISO/IEC 27000 series of security standards. While this is a laudable approach, it must be considered that compliance alone will not guarantee security [27].

The attack community are continually developing and exploiting new vulnerabilities, and thus a stringent and robust approach to system monitoring must be in place. There is little point in having a certificate to show compliance, if the company fails to detect a breach. Many breaches are not picked up until some time later. The risk emanating from this can turn out to be expensive. Recently, ASUS settled for $400,000 after they were sued by the Federal Trade Commission (FTC) [35], because they were not providing updates for their insecure routers. The new EU General Data Protection Regulation (GDPR) will come into force in May 2018. It will increase this (monetary) problem for companies with a maximum monetary penalty of up to 4% of global turnover.

D. Cloud Security

Often, companies will seek to prove they have achieved security through assurance. This assurance is usually achieved by compliance with standards, or by audit. However, one of the difficulties with cloud computing is that there are over 30 standards bodies who have been working on cloud security standards, and we are yet to see a fully comprehensive cloud security standard evolve [27]. There are difficulties too, with the method of compliance audit undertaken [36], which can have a considerable impact on the effectiveness of the audit exercise.

The fact that we have no complete cloud security standard is a major issue, meaning large corporates might be missing the potential to identify the increased risk arising from running their own software on the cloud. In the multi-tenancy, multi layer, environment of cloud computing, many forget that the solid corporate firewall they have so carefully developed for their corporate distributed systems does not extend to the cloud environment.

There is much we can learn from the approach taken by one of the most exposed market sectors to cyber risk — the financial services sector. This market sector is a prime target for cyber attacks. Liquid cash, particularly in electronic form is much easier to attack than large physical objects. Thus, in the next Section, we consider the approach taken to evaluating cyber risk in the financial services sector. These risks are well understood, and the risk models developed are now very advanced, and highly accurate.

III. Cyber Risk in the Financial Services Sector

Cyber risk has attracted increasing awareness for financial risk management in recent years. Financial intermediaries such as banks, investment companies, and insurance companies are the prime targets for cyber crimes. Figure 1 shows the average cost of cyber crimes incurred by companies of a specific industry, started from financial services, energy and utilities, and followed by defence and aerospace, and technology. The financial service sector has undergone a tremendous technological transformation, resulted from the adoption of digital banking, Financial Technology (FinTech), mobile applications, cloud computing, etc.

A. Cyber Risk in Financial Risk Management

It is of great importance to quantify cyber risk for financial risk management. Four types of risk - credit, liquidity, market, and operational — can affect the potential outcome / performance of financial investments for companies. Value at Risk (VaR) is a popular approach among modelling techniques used by financial institutions to quantify the market risk of investment. However, the model can not foresee a 'black swan event', a low-probability occurrence with high-value impact. Cyber VaR can be used to model the cyber risk, with consideration for cyber black swan events. A cyber VaR model can be used to estimate the likely loss of an organisation in the event of cyber attacks during a time period. The components of the VaR framework consist of the existing vulnerabilities of

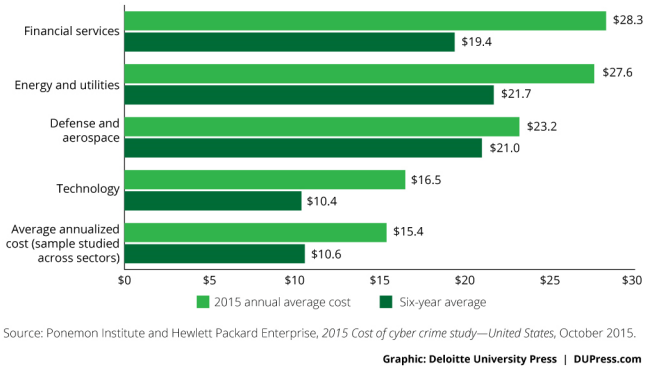

Fig. 1. AVERAGE ANNUAL COMPANY COSTS OF CYBERCRIME IN $MILLIONS

a system, the maturity of defending the system, the frequency of successful breaches, the tangible and intangible assets of the company, the types of attachers and their attacking motivations, etc. The adoption of cyber VaR can be helpful for a company to quantify the potential loss of a cyber attack.

B. Crypto-Currency in the Financial Sector

Crypto-currency, which is a form of virtual currency that uses crypography for security, may present increasing threat that negatively impact the cyber security of finance. Based on new applications of information technology, these virtual currencies attempt to remove money and banking from the control of sovereign governments, and they represent one of the most disruptive innovations ever in consumer finance. The underlying distributed ledger technology has many other potential applications in diverse areas such as property registration, accounting and auditing, gambling and financial derivatives.

The potential threat of this emerging technology motivates a better understanding of crypto-currency. It has essentially resulted from a technical experiment, with no monetary value. It has grown to an industry with more than 510 crypto-currencies with market value of $5.5 billion, composed of bitcoins. Although crypto-currencies have the advantage of higher efficiency and transparency for conducting transactions, reducing banking fees and bringing technological innovation to the financial industry, they are also used by cyber-criminals as they are not connected to any central banks and not regulated in many countries.

In the next Section, we explain why this model could be relevant to corporate cloud users.

IV. Why is This Relevant to Corporate Cloud Users?

In order to properly identify what risk is in the case of using cloud computing, users should first start with their prior evaluation of IT risk in regard to their existing distributed non-cloud setup. Since they will have been running these systems for a very long time, it is likely that the risks will be well understood. However, where a company assumes that because they understand these existing risks well, they will be well able to handle cloud risk, they will be placing themselves in considerable danger.

However, once they make the decision to move to cloud, simply moving software systems across to the cloud and assuming all past risks will continue as they have traditionally been identified, is a fallacy, and could lead them into a false sense of security. IT risk does not equal cloud risk. Any cloud ecosystem is far more complex than a traditional distributed IT system, and there are far more actors in the cloud ecosystem, meaning it is far more difficult to ensure a proper lavel of security can be achieved.

Many modern companies present an attractive target and will be subject to a raft of attacks, from a variety of different sources. These attacks will come from state sponsored actors, industrial espionage, hacktivists, specialist criminal gangs, and talented amateurs.

State sponsored actors will be exceptionally well resourced, will be very highly skilled, with the capability to breach systems, and leaving a minimal footprint. They are extremely hard to detect, and difficult to protect against, but may only be interested in keeping an eye on what the company is up to, in order to provide their government with the means to understand how other countries are progress in what may be a competitive market for their country. Thus, stealing cash is not likely to be high on their priority list.

Those who perpetrate industrial espionage generally have a view to getting their hands on new technology, either to sell to a rival, or to simply sell on the black market. They will generally be well skilled, independently well resourced from past espionage activities, and highly persistent. While that may have a long term impact on the company, they are less likely to be looking to steal cash.

Hacktivists are often very skilled, highly motivated towards their cause, although less well resourced than the previous groups. They usually are not concerned with stealing cash, but are concerned with exposing perceived wrongdoing by the target company. They are primarily motivated to cause maximum embarrassment, sometimes will seek to disrupt physical systems to highlight their cause, but generally are not interested in staling cash. Where they disrupt systems, the knock on damage could be substantial.

Specialist criminal gangs can range from well resourced and well skilled groups, down to small scale criminals, who will often “rent an attack” from the dark web. The primary goal of these groups is to steal cash, or to obtain intelligence, which will enable them to steal the cash at a later time. They tend to be very resourceful, highly skilled at social engineering attacks, and can often buy in the attack tools they require from the dark web.

The amateur group can range from very talented amateurs down to complete amateurs just trying to breach large systems in order to boast about it. The really talented ones are much harder to catch. While they can be very skilled, and have limitless patience and time to spend on the attacks, they often are poorly resourced, which can inhibit their activities. The

complete amateurs can be problematic from the damage they sometimes cause as they try to get into systems, or after they get there. The majority are not after cash, but the really talented ones can cause a huge amount of disruption.

So, with all these different actors constantly trying to get into company systems, why is the financial services sector of interest to cloud users? It is simply the fact that they have been targets of attack for a very long time, due to the very liquid nature of their business. Over the past decades, they have become very skilled in developing risk attack models to evaluate the risks they face, and are getting really good at it.

Equally, large companies often invest cash surpluses to maximise revenue production while they accumulate cash in preparation for their next expansion pus, thus in the process becoming greater targets. The attack actors have become adept at gathering a wide range of business intelligence in addition to learning how to analyse and understand financial statements, thus are able to pick better targets to attack.

Thus, companies must learn how best to evaluate properly they very real risks they face. In the next section, we consider how they might go about achieving this.

V. Finding the Balance

Risk is a fundamental part of any company. The main goal of any company is to maximise the generation of profit in a sustainable way. In order to achieve this goal, it is necessary to define what the target return will need to be. This provides the risk requirement needing to be accepted in order to achieve the desired outcome.

Assuming this risk requirement to be both practical and achievable, the management of the company will then evaluate all the risks in order to understand what they are taking on, not just to achieve the goals of the corporation, but to satisfy the requirements and obligations incumbent upon them, such as compliance with legislation, regulation, standards, best practice and accepted ethical standards of doing business. Enterprises need to be sustainable in the long run and resilient to shock. Each of these requirements can cause a conflicting pull on company management to ensure the best outcome can be achieved.

Not all risks must be taken by a company. Rather, they need to evaluate which risks to accept, which to mitigate, and which to decline, in order that they can satisfy all the requirements placed upon them. Clearly, some level of compromise will need to be made in order to find a suitable balance.

The best approach for achieving this balance is first to understand fully the extent of each risk, and to assess properly whether they are prepared, or need to accept each risk. By identifying those they must accept, if they understand the risk properly, they will be better placed to evaluate whether each risk should be accepted in full, in part, or rejected.

The use of a good evaluation model will provide a better means of achieving this goal more easily. This is why we suggest adopting the financial services VaR model on IT risk as a foundation for adapting it to also cover cloud risk.

VI. How Will it Work?

The application of cyber VaR would be of help to establish the minimum standard on covering the limits and risk assessment of cyber security. Based on the literature [37][38], the current challenge of quantifying and validating cyber VaR is the lack of quality data. Another shortcoming of the VaR measure is that it can be 'useless' for small probabilities with a significant outcome event. In finance literature, the Monte Carlo simulation and other measures have been proposed to tackle this. To address the impact / size of the outcome, the tail event or extreme event is defined as the largest percentage of losses measured relative to the respective VaR. Thus, the extreme event for cyber risk can be considered for risk management of cyber security.

VII. Conclusion

We have demonstrated how traditional and well understood approaches to IT security risk do not work well with trying to identify and evaluate cloud cyber risk. We have highlighted how cloud risks differ from traditional distributed systems, and illustrated weaknesses in existing approaches. We have looked at how cyber risk is tackled in the financial services sector, and suggest how adapting the proposed cyber risk VaR model might help to improve cloud cyber risk assessment, thus helping companies to find a better balance between risk and reward.

We note that the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance (CSA) have both introduced new updated approaches to cloud cyber risk. These and other national organisations are co-operating more with the ISO, who have produced a number of risk standards, such as ISO 31000 on corporate risk, ISO/IEC 27005 on information security risk management. We propose to review how their approach has been updated and will seek to discover whether any of these changes might be implemented into our system.

We are in the process of agreeing a plan to carry out a pilot development of this proposed system, and to compare its performance against existing approaches to evaluate how well it performs, with a view to providing the means of assessing the best level of risk awareness that is possible.

References

[1] Sox, "Sarbanes-Oxley Act of 2002," p. 66, 2002. [Online]. Available: news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf Last accessed: Jan 2017

[2] Crown, "Data Protection Act 1998," 1998. [Online]. Available: http://www.legislation.gov.uk/ukpga/1998/29/contents Last accessed: Jan 2017

[3] A. A. Berle and G. G. C. Means, *The modern corporation and private property*, 1932. [Online]. Available: https://books.google.co.uk/books?id=mLdLHhqxUb4C Last accessed: Jan 2017

[4] M. C. Jensen and W. H. Meckling, "Theory of the firm: Managerial behavior, agency costs and ownership structure," *Int. Libr. Crit. Writings Econ.*, vol. 3, no. 214, pp. 191–246, 2008.

[5] A. Cadbury, "The financial aspects of corporate governance," HMG, London, Tech. Rep., 1992. [Online]. Available: http://www.ecgi.org/codes/documents/cadbury.pdf Last accessed: Jan 2017

[6] M. C. Jensen, "The modern industrial revolution, exit, and the failure of internal control systems," *J. Finance*, vol. 48, no. 3, pp. 831–880, 1993.

[7] M. C. Jensen and D. Chew, "US corporate governance: Lessons from the 1980's," *Harvard Univ. Press*, no. December 2000, pp. 1–47, 1995.

[8] R. Greenbury, "Directors' remuneration - Report of a study group chaired by Sir Richard Greenbury," HMG, London, Tech. Rep., 1995. [Online]. Available: http://www.emeraldinsight.com/journals.htm?articleid=848139&show=abstract Last accessed: Jan 2017

[9] R. Hampel, "Committee on corporate governance," London, Tech. Rep., 1998.

[10] S. Turnbull, "Corporate governance: Theories, challenges and paradigms," *SSRN Electron. J.*, pp. 1–97, 2000.

[11] P. Myners, "Institutional investment in the United Kingdom: A review," HMG, London, Tech. Rep., 2001.

[12] H. Gov, "Transparency in supply chains etc. A practical guide," 2015. https://www.gov.uk/government/uploads/system/uploads/attachment _data/file/471996/Transparency_in_Supply_Chains_etc__A_practical _guide__final_.pdf Last accessed: Jan 2017

[13] R. Bauer, N. Guenster, and R. Otten, "Empirical evidence on corporate governance in Europe: The effect on stock returns, firm value and performance," *J. Asset Manag.*, vol. 5, no. 2, pp. 91–104, 2004.

[14] W. W. Bratton, "Enron, Sarbanes-Oxley and accounting: Rules versus principles versus rents," *Soc. Sci. Res.*, vol. 48, no. 4, pp. 1023–1056, 2003.

[15] K. Brickey, "From Enron to WorldCom and beyond: Life and crime after Sarbanes-Oxley," 2003. [Online]. Available: http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/walq81&section=19 Last accessed: Jan 2017

[16] B. Holmstrom and S. N. Kaplan, "the State of U.S. corporate governance: What's right and what's wrong?" *J. Appl. Corp. Financ.*, vol. 15, no. 3, pp. 8–20, mar 2003.

[17] L. E. Mitchell, "The Sarbanes-Oxley Act and the reinvention of corporate governance?" *Villanovo Law Rev.*, vol. 48, no. 4, pp. 1189–1216, 2003.

[18] R. E. Rosen, "Risk management and corporate governance: The case of Enron," *Conn. Law Rev.*, vol. 35, no. 1157, pp. 1157–1184, 2003.

[19] Financial Reporting Council, "The combined code on corporate governance," HMG, London, Tech. Rep. July, jan 2006. [Online]. Available: http://doi.wiley.com/10.1111/1467-923X.00209 Last accessed: Jan 2017

[20] Financial Reporting Council, "The Turnbull Guidance as an evaluation framework for the purposes of Section 404(a) of the Sarbanes-Oxley Act," Financial Reporting Council, London, Tech. Rep., 2004.

[21] G. Clinch, B. Sidhu, and S. Sin, "OECD principles of corporate governance," Organisation for Economic Co-Operation and Development, Tech. Rep. 4, may 1999. [Online]. Available: http://www.oecd.org/corporate/ca/corporategovernanceprinciples /33977036.pdf Last accessed: Jan 2017

[22] Financial Reporting Council, "The combined code on corporate governance," Financial Reporting Council, London, Tech. Rep. July, 2006.

[23] Financial Reporting Council, "Review of the 2003 combined code: Summary of responses to the review," Financial Reporting Council, London, Tech. Rep., 2006.

[24] Financial Reporting Council, "Review of the implementation of the 2006 combined code: Regulatory impact assessment," Financial Reporting Council, London, Tech. Rep., 2008.

[25] Financial Reporting Council, "The UK corporate governance code," Financial Reporting Council, London, Tech. Rep. September, 2010. [Online]. Available: http://www.nonexecutivedirector.co.uk/images/files/UKCorporateGovernanceCodeSeptember2012.pdf Last accessed: Jan 2017

[26] Financial Reporting Council, "The UK stewardship code," Financial Reporting Council, London, Tech. Rep., 2012.

[27] B. Duncan and M. Whittington, "Compliance with standards, assurance and audit: Does this equal security?" in *Proc. 7th Int. Conf. Secur. Inf. Networks*. Glasgow: ACM, 2014, pp. 77–84.

[28] J. W. Barnard, "Shirking, opportunism, self-delusion and more: The agency problem today," *48 Wake For. Law Rev.*, pp. 745–770, 2013.

[29] B. Duncan and M. Whittington, "Company management approaches — stewardship or agency: Which promotes better security in cloud ecosystems?" in *Cloud Comput. 2015*. Nice: IEEE, 2015, pp. 154–159.

[30] N. M. Brennan and J. P. Conroy, "Executive hubris: The case of a bank CEO," *Accounting, Audit. Account. J.*, vol. 26, no. September, pp. 172–195, 2011.

[31] ISO, "ISO/IEC 27000:2009," 2014. [Online]. Available: www.iso.org

[32] IT Governance Institute, *Cobit 4.1*, 2010.

[33] PCI Security Standards Council LLC, "Data Security Standard: Requirements and Security Assessment Procedures," PCI Security Standards Council, Tech. Rep. November, 2013.

[34] PWC, "UK information security breaches survey - Technical report 2012," London, Tech. Rep. April, 2012. [Online]. Available: www.pwc.comwww.bis.gov.uk Last accessed: Jan 2017

[35] FTC, "ASUS settles FTC charges that insecure home routers and "cloud" services put consumers' privacy at Risk," 2016. [Online]. Available: https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put Last accessed: Jan 2017

[36] B. Duncan and M. Whittington, "Reflecting on whether checklists can tick the box for cloud security," in *Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom*, vol. 2015-Febru, no. February. Singapore: IEEE, 2015, pp. 805–810.

[37] C. Biener, M. Eling, and J. H. Wirfs, "Insurability of cyber risk: An empirical analysis," Geneva Pap. Risk Insur. Issues Pract., vol. 40, no. 1, pp. 131–158, 2015.

[38] P. Pandey and E. A. Snekkenes, "A performance assessment metric for information security financial instruments," in Information Society (i-Society), 2015 Intl. Conf. on, 2015, pp. 138–145.