Good Governance in the Age of Collaboration

The three pillars of corporate governance - transparency, accountability and security are constantly evolving concepts. Good governance is never a task complete, as it needs to be a developing set of principles in order to meet the demands of modern business as it changes too. As new challenges emerge, new risks appear to the fore and the bar for excellence is constantly raised, a fresh approach is always needed.

Good governance requires constant evaluation as to whether the current processes and principles are enabling organisations to perform optimally and to achieve sustainability. However, it is even more pertinent to evaluate the current approach to governance in light of the age of collaboration. This essay will focus on the challenge of governance in the age of collaboration and how this is an example which calls for a fresh approach to a number of core principles of corporate governance. This question will not be answered by referring to old concepts with a binary solution. Rather the answer lies in how good governance maximises collaboration with employees to create practical and innovative plans for good governance. This essay will first consider the current corporate governance approach including the role of the employee, secondly a discussion of the challenges facing good governance in the age of collaboration and finally the need for a fresh approach in order to meet these challenges.

The Current Approach:

Security is one of the greatest concerns for good governance today. Unique risks have emerged in recent times which require a new way of thinking and a new approach. Cyber threats are multi-faceted risks that involve a multitude of actors, concerns and motivations. They have developed from the "Morris" computer worm in the late 1980s,[1] to hacking for fame,[2] to becoming one of the greatest concerns of 21st century business.[3]

The governance approach that pervades today is so often to focus is on building walls high enough to keep the 'bad guys' out. Focusing on the motivations of hackers whose inspiration is to gain a financial advantage, or hacktivists seeking revenge against corporations or even on international hackers engaging in espionage automatically turns the tone of the discussion

[1] DTCC, "Cyber Risk – A Global Systemic Threat", [2014].
[2] *Ibid.*
[3] Lloyd's, "Managing Risk in the 21st Century", [2015].

sinister.[4] However, often the greatest risk is in fact posed by the individuals who hold this valuable information – employees. When the boardroom discussion turns to this topic the tone can become prophetic.[5] Rather than focusing on best strategies discussions turn to the malicious and vengeful employee – aligned with the same mal-intent of the hackers. Therein lies the fundamental challenge of businesses today when addressing issues of keeping company data safe. The greatest threat is not those motivated by ill-intent. Those are a secondary concern. The greatest threat to most businesses is posed by a lack of awareness, knowledge and education in order to keep business information safe and avoiding data leaks. This is a strategy lacking in many corporate governance strategies today – still focused on approaches ill-suited to the current workflows of many businesses.

There has always been a debate as to the role of the employee in corporate governance. The balancing of interests of many stakeholders is a core pursuit of corporate governance. How employees can help with this pursuit in the 21st century is of ever growing importance. In Germany the role of the employee is of great importance, with employee representation on the supervisory board being common and in a number of circumstances legally mandated.[6] The rationale is that the first-hand experience of employees and their operational knowledge assists corporate board decision-making.[7] A common trend internationally has been the transition from detached supervisory boards, such as those studied by Edwards and Fischer, to boards engaged in active monitoring of management and firm performance.[8] This further drives the need to refer to employees to gain an insight into daily performance and how best to optimise processes. There is a debate as to the optimal corporate governance balance. This debate is greatly welcomed, however these writings are still only emerging, and the role of employee representation in governance is even less developed.

Collaboration Age:

A core feature of any successful business today is the ability to rapidly share ideas, news and work. The ability to collaborate easily is in the DNA of every business today. The amount of

[4] PWC, "Safeguarding Your Firm from Cyber Attacks", available at <https://www.pwc.com/us/en/law-firms/assets/pwc-safeguarding-your-firm-from-cyber-attacks.pdf>.
[5] Thomas J Harvey, "Battling Employee Sabotage in the Wired Workplace", Center Collection [2001].
[6] Rebecca Page, "Co-determination in Germany", Arbeitspapier 33 [2009].
[7] *Ibid.*
[8] Grit Tüngler, "The Anglo-American Board of Directors and the German Supervisory Board - Marionettes in a Puppet Theatre of Corporate Governance or Efficient Controlling Devices?", BLR Vol. 12 [2000].

data that businesses are responsible for on a daily basis is huge and continually growing. Laptops, iPads, phones, control systems, applications, software make up the fabric and identity of a company, all being interlinked and controlled on varying levels. In doing so, businesses open themselves up to a wide variety of machines and lose direct control of data security. While at the same time, becoming increasingly dependent on IT.

Looking even more to the future the internet of things. This will mean an increasingly connected working environment. Collaboration across platforms from not just people sharing information but physical devices such as home appliances and cars to the internet. People logging in and out of their office. Their coffee machines, computers, even music being set up to play at a certain time. The comings and goings of people in the office not by mere human observations but by that information being continually, systematically and dutifully logged. Currently coined the "Internet of Vulnerabilities," by cyber experts.[9] This ignores one of the greatest possibilities of the 21st century. However, it does show case the vulnerabilities that can be found within a business when one examines how businesses can rapidly share such huge volumes of information now and in the future. The reality is that the abilities of businesses to manage this on the highest level and develop strategies and plans does not operate at the same speed.

Fresh approach: Acknowledging the Working Reality of a Company:

With the democratisation of IT, employees ever increasingly taking it into their own hands how they choose to work. If their voices are not heard they will continue to use the tools they find easiest and most user friendly. In the “bring your own device” era the line between what tools you use, device and how data is managed becomes even more blurred. Couple this with the ever growing need for collaboration and this means that increasingly businesses struggle to keep hold of their information in any systematic or centralised way. Fighting this shift in mentality will only get businesses so far. The more reluctant businesses appear to their employees, to be willing to consider new tools, the more employees will bring these tools underground and away from the gaze of IT. In turn, this makes it ever more difficult for businesses to tackle the greatest risks within their businesses on a daily basis. Therefore, in

[9] Grobauer, B, Walloschek, T, Stocker, E, “Understanding Cloud Computing Vulnerabilities” [2011] *IEEE* 2(9).

modern practice a huge divergence appears between the decisions of the board as to what is good governance and the practical reality of how these processes are being implemented in practice – if at all.

Businesses operate in an incredibly interconnected system. Therefore, protecting the business against cyber-attack is not just a project to protect internal systems but rather to think about the tools businesses use on a day to day that is managed by third parties and the third parties that they do business with. The ability to shield a business against data leak is only as good as the tools used and the people businesses work with externally as well. The information that is sent out from a company or put in the hands of third party service providers is therefore only protected to the extent that these third parties shield data from cyber-attack. This is not an argument to operate as an island in business, indeed this is impossible. This is a point as to why internal policies should not just look at internal systems and sharing relationships that are officially mandated by IT and the business on paper. Rather this requires businesses to look at the tools that employees are actually using. Creating an open environment where these points are being discussed with employees rather than employees being dictated to by the board as to what is the official policy rather than the workflows that are reflected in reality.

One of the most prevalent problems within businesses, and thus one of the greatest risks, is managing documents and ever moving data. In terms of collaboration tools such as Google Drive, One Drive, Dropbox and Box the challenge is that boards see these tools as a potential vulnerability and see individual employee's accounts as being open to data leak. These fears derive from a couple of the most basic principles of corporate governance - one being accountability and the other security. Of course, these are both principles that continue to offer continuing assistance in good governance. However, in the collaboration era accountability comes into conflict with the current approach to governance of most corporations. Methods of work are constantly changing. Therefore, it is difficult to always know what is the safest and most secure tool to use. Accountability can denote answerability or liability. In the matrix that exists between multiple stakeholders, individuals are very interested in who will take the blame when something goes wrong. This is an understandable concern that traces back to financial scandals in the early 2000s.[10] Of course, accountability means more than that. It also means ownership over one's actions when the consequences of those actions are good. However, where there is no obvious correct choice and no well-trodden path it can appear that only

[10] David A. Katz, Wachtell, Lipton, Rosen & Katz, "The Changing Dynamics of Governance and Engagement", Harvard Law School Forum [2015].

negative accountability may result. Coupled with governance policies that are traditional conservative when it comes to concepts of security, as opposed to pro-active in seeking emerging solutions, the shift that is needed in concepts of governance can seem mammoth.

A simple ban mandated by the board ignores the need that employees have for flexible tools such as this and instead of taking control, push control further away from sight. Distinguishing between the consumer versions of these products and the enterprise versions shows the multifaceted and thought out approaches IT teams need to make in order to protect businesses against cyber-attacks. Therefore, the need is to look to the future in building a safe and secure system rather using blank tools like shutting tools down or seeking to contain it ignore the reality of how employees are working. Instead this results in a cyber policy that does not reflect the commercial reality of a company.

Of course, the point in response to this is that the official decision, mandated by the board, to outsource IT and technology platforms to third-parties invites a host of new legal issues that may have significant risk management ramifications. This is a risk that businesses are not willing to take. Indeed, recent cases focusing on aspects of the EU wide protection for data, such as Safe Harbour, does mean that businesses increasingly do not know what official policies they should adopt or look to in this ever changing landscape.[11] The reality is that increasingly it is impossible to manage every aspect of a businesses' data internally. Businesses cannot create a bespoke system to the same standard as technology companies that focus on this twenty-four hours a day. Most businesses will not be able to put in place a bespoke system because most of those bespoke systems have to periodically adapted to be compatible with any other software they use that may disrupt its operation. So externality is really a necessity. To argue the converse feels like saying do not go to the bank, sleep with the money under your mattress. The power in fact lies in control and choosing how to manage a workflow that does exist rather than ignoring it. Therefore, the idea of this essay is not to suggest that businesses adopt every tool and practice unofficially developed by their employees, but rather that boards have a pro-active process in place to discuss openly the possibility of internal change and bringing unofficial practices above ground.

There are ten global principles of corporate governance.[12] When it comes to the age of collaboration for businesses a fresh approach is needed with regard to a number of those core

[11] *Maximillian Schrems v Data Protection Commissioner* C-362/14 [2015].
[12] Corporate Governance Code, the Australian ASX Corporate Governance Principles and the South African King Report.

principles. In particular: transparency and integrity of the information provided; cooperation between employees; respect for formalities; independent controls and supervision; voluntary accountability and importantly sustainability and long term perspective in the conduction of business. The age of collaboration for business and touches upon all those questions. A fresh approach is needed in order to re-evaluate the very purpose of corporate governance. That being to lead and develop processes that look to the long term perspective of business, rather than being overly reluctant in acknowledging the rapidly developing working reality of a business.

A 21st century approach to good governance will not be achieved by a handful of key stakeholders, it will be won by a more inclusive approach seeking collective plan of response. It needs to be a topic where every player in a company feels like they are the custodians rather than a handful of IT staff. To do so requires leadership. This starts at the very top but what is most critical is that the end user feels empowered and educated in how best to protect the business. Combatting data leak will be won by having a clear policy which reflects the working reality of a company so that the organisation has absolute oversight on what data is being shared at a company-wide level. The fundamental point here is this, even though these cyber risks are complicated and intricate the solution can be as simple as common sense. Employees often hold the solution here to data breaches.

They are the front line.

Without them the war will be lost before even entering battle.