THE NEW GOVERNANCE PARADIGM: THERE IS RISK, AND THEN THERE IS TECHNOLOGY RISK

THE NEW BOARD OVERSIGHT PARADIGM

There is no doubt that when directors look back at the last two decades, it is quite clear that board governance has changed. From passive approval, to engaged decision making, all boards are working on their roles with much greater intensity and much greater focus, than ever before.

Sarbanes-Oxley legislation forced boards to change their perspective and actions; and now changes in the external environment are changing board members focus. If we look at the three "standard governance committees" of the board, we find that each has changed dramatically. The Governance Committee has morphed into true Nominating and Governance functions, and they are exercising meaningful control over the board staffing and the board governance process. And, most Governance Committees are working diligently to be certain that they exercise the best processes by implementing best practices, and even getting external organizational support to help them elevate their own functioning through governance training and even board performance evaluation.

Audit Committees were clearly directed to "take control of the Audit Function" and they have. In opposition to the past, they now "own" the relationship with the public accounting firm, and they are clearly acting in an independent manner with respect to financial management. They have direct relationship with the public accounting firm, and they "hire and fire" that supporting organizational entity.

Compensation Committees have come to recognize that the public shareholder holds them accountable for the compensation perceived excesses for executive compensation. The scrutiny that they have endured over the last several years has forced them to be far more aggressive in managing the independent consultants used to evaluate compensation options. Those consultants now "work for the compensation committee."

Thus, the key factors of financial controls and executive compensation are being managed by committees of the board. This is not because the board views them as unimportant, but because the board knows that there are technical factors that require board members to understand and know the key issues around these factors. In short, these committees may be knowledgeable, but they have experts who support them.

THE CHANGED ROLE OF TECHNOLOGY IN YOUR BUSINESS MODEL

At a time when most board members began their corporate careers, technology was a process enabler. Back then, the role of technology was to "automate" existing processes. The "Systems & Data Processing" officer was typically charged with taking an existing manual system, and creating programs that would do computations or process thousand of items, more quickly, by "automating the process." Go back far enough, and implementing technology was to take piles of "punched cards," and convert the data contained in them into digital records on magnetic tapes.

In very few organizations, was technology at the core of the business. More importantly, virtually none of the processes were dominated or controlled by a computer. Technology supported the staff actually doing the work.

Fast forward to the current day; where technology plays a dramatically different role: Consumers buy products "online," without the intervention of a single human action; assembly lines, using robots, manufacture/assemble finished goods; manufacturing control systems manage the entire process, from raw materials to the logistics of getting the product to the buyer; decisions are not just enabled by technology, those decisions are made by the deployed software; data bases are not just expansive, big data analytics manipulate Terabytes of data to analyze consumer behavior; ATMs, handle the entire check cashing and deposit taking function for banks; payment systems can eliminate the use of cash and credit cards, through consumer electronic payment vehicles; health records are becoming entirely electronic, replacing huge file cabinets of paper files, and those records are available through networks to a variety of interested professionals; computers are connected to other computers through network technology; the emerging "internet of things," connects some of the most mundane physical products to control systems that monitor their performance; and finally, automobiles are, and increasingly will be, navigated by electronic systems, replacing the human driver.

This list could be multiplied by an order of magnitude, and still would not be complete. When Tom Watson Jr. decided to build the IBM System 360, probably the first truly commercially viable computer, it is unlikely that he ever contemplated how pervasive, the "digital revolution" would become. Yes, we have talked about the "Industrial Revolution," as having transformed the manufacturing model, but the simple fact is that we live in a digital age, and virtually every aspect of every activity in our lives is influenced by, or controlled by, the digital technology.

But, that "digital technology," was really only the start. Another revolution occurred, and that revolution has not only transformed what we could achieve with digital technology; but also it has changed the business model of virtually every company in existence. That new technology was the advent of Networking on a broad and expansive scale. This paradigm shift has changed the business models of practically every company in the US, and will continue to drive the future strategic direction of virtually all. The creation of the World Wide Web, and what we generically refer to as the Internet, has changed everything, and probably will continue to do that forever.

THE BRAVE NEW WORLD IS HERE

In a recent board consultancy session, one of the participants tried to make the case that information technology, data security, information security and Cyber Security hacking threats were simply another risk that needed to be managed by the corporate Risk Management process. Indeed a few days later, a panel discussing Cyber Security restated that Cyber Security was serious, but it was simply another risk that needed to be managed by the Enterprise Risk Management function. They did not try to minimize the

importance of the Cyber risk, but what they argued was that Cyber Security needs to be an integrated part of the entire ERM, and that it was serious, but needed to be put into perspective. In point of fact, it is important to note that, these risks must be incorporated into the Enterprise Risk Management process. To not do that, would be shear negligence.

During the last two years alone, I have spent over three hundred hours in boardrooms discussing these threats with full boards, Audit Committees, Risk Committees, Lead Directors and concerned individual board members, and I believe that I have put the threats into "perspective." I believe that this package of issues is the single most significant threat/risk facing virtually every business. Indeed, I believe that it is an "**Existential Threat**" to virtually every type of business today; and, that by allowing it to be handled only by the routine ERM process, will eventually allow the "bad actors," to put your company at risk…by not just having a technical problem, but to have its very existence threatened.

Most members of the military, intelligence or criminal investigations community do not believe that this is "just another risk." Most military personnel are beginning to believe that the next military conflict of nations states will be largely conducted in "cyber space," not "on the ground" with infantry. Yes, we need to worry about conventional and nuclear weapons; and, yes, we need to be focused on ground invasions by warring parties; but, we need also to be aware of the daily threat posed to government, military, business and individual operating systems, by a series of "threat actors," who all want to have access to your intellectual capital and key non-public information. These "threat actors" include independent hackers; thieves, corporate espionage artists and nation states with a desire to gain access to our critical infrastructure and our intellectual capital.

Conventional wisdom used to be that all organizations were at risk for having a "bad actor" hacking attack. Today, conventional wisdom is that your organization has already been attacked, and that it is almost certain to have been the victim of one or more hacking protocols that left behind either current damage, access to accomplish future damage to your data files, or as has already become obvious, to have stolen data from your most important data base of customer information or intellectual property.

NEW PARADIGM: NEW DEMANDS: UNPREPARED STAFF AND BOARDS

So, what are the lessons learned here? The key factor is that boards learned to delegate key issues to committees charged with the role of oversight over the complex or technical areas of Audit, Compensation and even Governance all qualify as critical oversight responsibilities, where technical capacity is required to accomplish the oversight role.

Let's take a look at other oversight roles: Strategy, Marketing & Sales, Customer Service Operations, even Operational monitoring. These are essential functions, but they are also generally routine business activities, where most boards have core competence in the rest

of their professional lives. Most boards feel competent in the reviewing and monitoring of these.

On the other hand, how many board are actually competent on reviewing and approving Information Technology issues? Further, how many firms have operations that are not clearly connected to the technology deployed? In many ways, there are very few firms in the market where IT is a "side bar " to the business. More often than not, Information Technology is at the core of the "business model." And if it is not at the core, it is very high on the risk profile of the enterprise.

Seldom today will you find a board that is not challenged by Information Technology threats. They may be as simple as inadequate resources committed to aging, legacy technology that requires massive updating; to the most serious, "threat actor" penetrations that damage core, non-public customer data. Worse still, could be the ability of a "threat actor" penetration that legitimately closes down the operations of the company. These operational threats could mean, destroying the data bases entirely; to disabling the networks used to communicate within the company; to enabling physical access to facilities, by disabling all security systems; to destroying the operating systems processing routine transactions; to even shutting down an operational system by shutting down the entire power grid; In short, the risk of unauthorized and malicious penetration is huge, and the challenge of managing it is even greater.

Also, management is not immune as it has huge challenges in protecting against these penetrations, let alone how it responds when a serious breach occurs. In short, the entire company can be at risk by virtue of a simple intervention by malicious hackers, to serious intentional destruction by thieves or even malware deposited and designed to destroy companies that could be planted by adversarial nation states. In short, even the best of managements are struggling to staff these functions. *The board oversight function is seriously weak in its ability to review, monitor and govern these risks.*

So what can a board do to exercise its oversight over technology risk and data security? The current model is that the board as a whole, or the Audit Committee, or even the Risk Committee will have general oversight over these challenges.

A NEW GOVERNANCE MODEL IS REQUIRED

The simple fact is, virtually every board today is seeking help in this area. The first perceived "fix," is to attempt to recruit board members with Technology backgrounds, who can bring their technical experience to the board. The further truth is that as boards seek this talent, they also discover that the average "technically qualified" board prospect may have very little general management or board exposure or experience. It sounds great to search for Chief Information Officers (CIO's) who can become board members, but most are preoccupied with their own corporate risks, and few have had the experience in board governance. The search should go on, but even with that core technology background, most boards still have a gap in their ability to both comprehend the issues, and to have a meaningful oversight accomplished.

This lack of technical expertise is precisely what caused the Audit functions of many organizations to be too weak to prevent many of the pre- Sarbanes-Oxley crises faced by corporate America. Much to the chagrin of many, it actually took federal legislation to force boards to look at the Audit function with a different, and more technical perspective. Audit Committees of pubic companies today are expected to have at least one "financial expert" on the Audit Committee, and the relationship between the Audit Committee and the Internal Audit function clearly made the direct reporting of that person to the Audit Committee mandatory. Further, the external Auditor in essential all cases today, public or private, is a direct report to the Audit Committee. The sense of independence of these two roles has created an unambiguous independence on their part, and they each act in consort with the needs of the Audit Committee. In a similar way, the Compensation Committee has found itself reliant on independent expertise to support the very technical aspects of Executive Compensation.

So, that leads us to this highly technical area of Technology. If these kinds of independence and technical support are considered appropriate for internal financial controls, then why not for the core technology that drives not just the financial accounting and reporting, but drives, even controls all of operations? Long gone are the days when we called this function Systems and Data Processing; the Chief Information Officer ; the Chief Technology Officer or whomever that role might be, is no longer just processing widgets in the organization; that person now has management oversight over the "intellectual capital," of the enterprise, and the technology used today is dramatically different and substantially more complex than anything envisioned two decades ago.

So if that role has gotten more complicated, then so has the board's need to have oversight. Further, there is so much risk in managing data security that the Chief Information Security Officer (CISO), in many ways holds the keys to the "crown jewels" of the company. With all of this, the board has no real place to turn.

SO, WHAT ARE WE TO DO?

We believe that the answer is that there is a need for a Fourth Standing Committee in every public and private company. We now have Audit, Compensation and Nominating & Governance. Our view is that a fourth, a Data & Technology Committee is required. This Committee should be staffed with operationally-based board members, at least one of which can be designated a Technology Expert; and the Committee must have reporting to it, both the CIO and the CISO; and it must have an outside technical resource in the form of a Technical Support Advisor who is qualified to provide Information Technology and Information Security Reviews and Audits. In short, this Committee needs the same type of independent support from outside advisors as the Audit and Compensation Committees have today.

This new Committee must be charged with all the same types of auditing, testing, verification, review and validation processes that the current Audit Committees have over the system of internal controls. This Committee must be able to look to the external

advisor to assure itself that the project management and information systems architecture will support the strategies of the company, and that the information and data security processes are robust enough to maximize the protection against data breaches and threat actor penetrations. It must also be in a position to do audits of the data security programs, validate the effective use of data security tools, and be in a position to evaluate the data breach response plans and the ability of executive management to execute them.