By Scott M. Shemwell, D.B.A.
Managing Director
The Rapid Response Institute

A Governance Model for the Era of Digitalization

Achieving Operational Excellence Using Disruptive Data Management Techniques

At a recent conference, one of the panelists (an investment banker) when referring to the so-called *digital oilfield* suggested words to the effect that if the enterprise is driven by these technologies then it is now an agenda item for the Board of Directors. We raised this issue several years ago before some of the major visible incidents, i.e. *Deepwater Horizon*. With appropriate governance, operational failures may not have happened. At a minimum, their impact could have been mitigated and the response more rapid – Systemic High Reliability Management.

At that time, the idea was largely ignored. IT was an enabling tool, sometimes outsourced and not considered part of the core competency of the firm. Is IT now a core competency?

The term governance is often poorly understood. This is particularly true when it comes to the subject of Information Technology.

Contemporary Governance

Modern enterprise governance evolved as a function of financial reporting and the need to uncover fraudulent behaviors. Readers will remember that at the beginning of the century, the behavior of firms such as Enron, MCI, Tysons and others led to the Sarbanes-Oxley Act of 2002 (SOX) and its regulatory requirement for greater transparency of financial reporting processes.

Earlier governance models include the 1985 formation of the Committee of Sponsoring Organizations (COSO) with the mission to provide leadership in enterprise risk management, internal controls and fraud detection for the private sector. The COSO framework continues to evolve as new threats emerge.

While these models profess enterprise level of governance at the CEO, CFO and Board of Directors level, they often fall short at the operational level. A 2012 study of the Operations Management Systems (OMS) rolled out post the 2010 *Deepwater Horizon* disaster, revealed major governance gaps at the operations and contractor management level. Many of these identified issues remain.

Historically, IT Governance has been defined from the perspective of the CIO and her requirements to Align IT with the Business, Attain Better Efficiency, Reduce Costs and Process Cycle Time and Improve Overall Quality, etc. This has led to a number of shortcomings in the implementation of software applications, bug fixes and other "IT driven" initiatives.

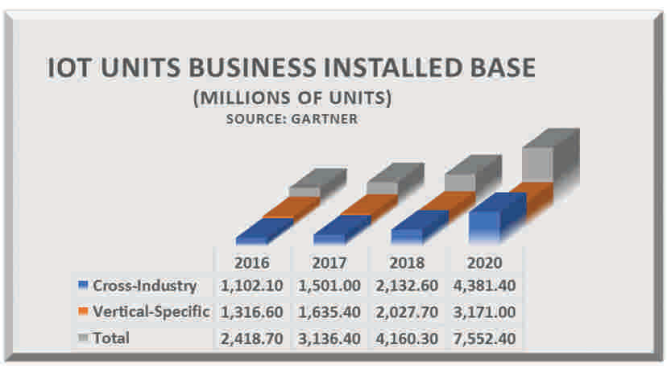
One of the more notable failures of this governance model is the cyber-attack on the US credit reporting firm, Equifax in May of 2017. This successful cyber-attack lead to the resignation of several key executives including the CEO. According to reports, the firm was aware of this vulnerability and had possession of the "bug fix" yet failed to update its system in a timely manner.

The resulting breach potentially impacted the personal data of upwards to 143 million individuals. The ultimate impact of this failure has yet to be determined.

Other high profile 'hacks' continue to occur with seemingly higher economic stakes each time. Clearly, the current IT governance models for many major global organizations and governments are broken.

The IT research firm Gartner forecasts Industrial Internet of Things (IIoT) devices will proliferate exponentially. The installed base should exceed 7.5 billion by the end of the decade.

As shown in the figure, there are two categories of IoT. Vertical-Specific devices include those that are used in manufacturing/production processes as well as other real-time and offline devices necessary to generate revenue. Cross-Industry devices are defined as those that support the enterprise, i.e., HVAC, physical security, etc.



	2016	2017	2018	2020
Cross-Industry	1,102.10	1,501.00	2,132.60	4,381.40
Vertical-Specific	1,316.60	1,635.40	2,027.70	3,171.00
Total	2,418.70	3,136.40	4,160.30	7,552.40

Moreover, the number of smartphone users is expected to grow by an additional half billion to almost three billion in 2020. One would expect that a significant number of these devices will be used in commerce as well, i.e. operations management, online procurement, testing, etc.

In addition to ERP systems and many enterprise applications such as Drawing and Document Management, Asset Integrity Management and literally thousands of current and future software and Software as a Service (SaaS) solutions, it is likely that over 10 billion individual devices will enable global commerce. This will present a monumental challenge to not only grow stakeholder value but secure it from maleficence as well as possible user incompetency, i.e. poor password management.

Emerging Model

The consulting firm McKinsey projects that in the current (and foreseeable) commodity price trading range that oil and gas operators must "reinvent" themselves if they are to remain productive and competitive. We have already seen some of this with the US Shale producers with their deployment of new directional drilling and fraccing technologies.

The firm identifies three major areas where digitalization can add significant value to the enterprise:

1. *Operations of the Future* – perhaps the next generation of the digital oilfield, with a focus on maintenance and equipment reliability. This may account for 25+ percent savings in operating costs.
2. *Reservoir Recovery* – the use of imaging modeling solutions that can increase production up to 40 percent.
3. *Digital-Enabled Ecosystem* – the optimization of the supply chain lowering cost up to 10 percent.

However, what is digitalization? Some define it as the machine-to-machine interactivity often called the Industrial Internet of Things. Perhaps, it is more.

There remains a high level of human interactivity with machines and among individuals themselves. Volumes have been written regarding the need for greater collaboration among global teams, including contractors and their subcontractors.

A broader definition includes the use of data and information in *decision-making processes* whether human or machine, i.e. process control. In other words, Human Systems Integration (HSI).

From a forthcoming book by this author and his co-author; "HSI considers the following seven domains: Manpower, Personnel, Training, Human Factors Engineering, Personnel Survivability, Habitability, and Environment, Safety and Occupational Health (ESOH). In simple terms, HSI focuses on human beings and their interaction with hardware, software, and the environment."

Simply, HSI harnesses the disruptive power of digitalization and focuses it where the highest value can be extracted. As with most advances, it is how the human applies it rather than the technology itself that provides a sustained advantage.

The initial hypothesis herein, "if the enterprise is driven by these technologies that it is now an agenda item for the Board of Directors" requires an updated governance model. The implication; competitive advantage and even survival of the firm now rests on information technology more so than the technologies that previously led shareholder value growth, i.e., manufacturing, logistics, engineering etc.

The COSO model has evolved and been updated on several occasions since its inception in 1985. In June 2017, its current version titled, *Enterprise Risk Management – Integrating with Strategy and Performance* was released.

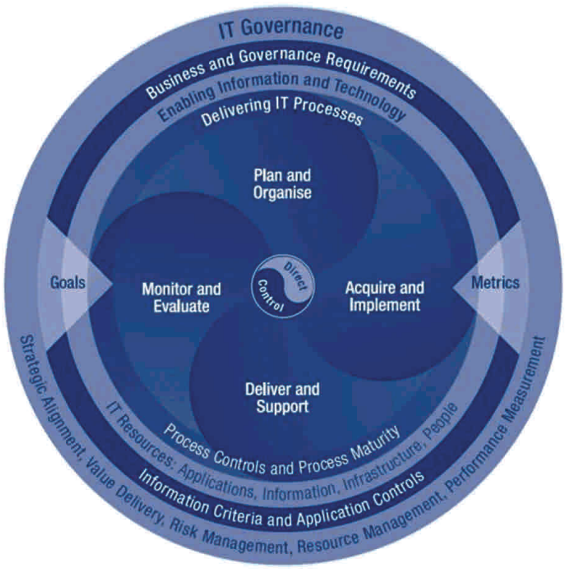
As expected by the name, there is increased alignment between strategy and performance. This includes, "Evolving technologies and the proliferation of data and analytics in supporting decision-making." Other areas of expansion include a recognition that the global business environment is increasingly complex and that there is a need for operational harmonization across all markets served. Enterprise Ecosystem Risk Management remains at the core of this enhanced framework.

Strong Bond Governance

In our 2014 book, *Implementing a Culture of Safety: A Roadmap for Performance Based Compliance*, we put forth the construct of Strong Bond Governance. Basically, "The Culture of Safety started with an anchor at the Board of Directors level."

This thought leadership was an early stake in the ground that the legacy governance models were no longer applicable. Today, digitalization is a Board of Directors issue, perhaps more so than financial transparency or the audit committee. Bet your company and bet your personal reputation!

The following figure depicts the ISACA CORBIT 5 Governance Framework that aligns the business for the enterprise governance of today's information technology. ISACA indicates that the model is built on ISO and other industry standards and appropriate for organizations that are either transitioning or sustaining a digitalization initiative.



From this pundit's perspective, the core of this model is Strong Bond Governance. The yin and yang of Direct presence and Control are at the center of four key processes and their goals and metrics. Layers of enablers and requirement focus on the strategic alignment of IT Governance.

This model is a step level change from legacy IT Governance. However, it does appear to still have its main focus on the technology as opposed to the business.

One approach is to develop this aspect of the overall enterprise governance within the structure of the new COSO model. If digitalization is transforming the enterprise, the governance models must reflect the renovation. If they do not, then the full value many believe is available may not be realized.

Going Forward

Cyber-attacks appear to be the gift that keeps on giving – see *Cybersecurity 2017—Trends and Issues to Sustain High Reliability in the Oil & Gas Sector: Develop a Cybersecurity Framework for Your Enterprise, Petroleum Africa, January/February 2017*. Weeks after Equifax 'sat' on the release of information regarding their mega breach, it appears that the new CEO of Uber did the same thing for two months – another 57 million accounts compromised.

SOX and other regulations demand transparency as a function of the fiduciary responsibility of executives. Studies have shown that greater transparency can increase the common stock price of publicly traded companies? If these statements are correct, why is yet one more firm withholding information regarding "digitalization failures" that investors (and regulators) have a right know?

Are these seemingly intentional lapses in transparency SOX violations? If so, what are the repercussions for these CEOs and their Board oversight committees – board in general too? Clearly, IT Governance alone is not sufficient! This is in arena of a moral imperative.

The economic and personal costs of these continued cyber-attacks is staggering. And with no slow down or seemingly adequate defense, the digitalization business model and value expected is at risk.

According to the World Economic Forum, "Digital transformation in the Oil and Gas industry could unlock approximately $1.6 trillion of value for the industry, its customers and the wider society." This number is beyond massive or even game changing.

It is the opportunity to completely remake this sector. Significant stakeholder value is available to all economic actors. If an organization does not capitalize on this opportunity, is this management malfeasance along the lines of Enron?

The rising digitalization tide can lift all organizational boats. Lower cost, better safety and higher earnings per share are only a few of many value add metrics.

Operational excellence demands no less. However, without this new governance model, operational excellence is unlikely and other organizational and personal pitfalls identified herein have an increased likelihood.

The term 'likelihood' is a common metric used in most risk management models. In other words, risk goes up when the likelihood of detrimental impacts increase.

Implemented well, the digitalization value proposition is almost without limits! Finally, this value is available to all economic actors in the sector regardless of size or locale.

About the Author

Dr. Scott M. Shemwell, sshemwell@theRRInstitute.com, Managing Director of The Rapid Response Institute, and CEO of www.OARS360.com is an acknowledged authority and thought leader in field operations and risk management. He has over 30 years in the energy sector leading turnaround and transformation processes for global S&P 500 organizations as well as start-up and professional service firms. He has been directly involved in over $5 billion in acquisition and divestitures as well as the management of significant projects and business units. He is the author of six books and for over a decade, he and his firm have helped clients adapt to the dramatic changes impacting the global energy and heavy industry sectors. www.theRRinstitute.com.