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

Assuring the Enterprise is Cyber Secure

Enterprise Digitalization/Internet of Things and the Operational Driven Bottom Line

The subject of cybersecurity remains somewhat of an enigma in the oil and gas sector. Even many who hold themselves out as experts in the digital oilfield have a weak perception of the threat a digital enterprise faces from cybercrime.

In the January/February 2017 edition of *Petroleum Africa*, "Cybersecurity 2017 – Trends and Issues to Sustain High Reliability in the Oil & Gas Sector: Develop a Cybersecurity Framework for Your Enterprise", we identified several critical areas of concern. These include the ubiquitous nature of cyber-attacks, the need for involvement by the board of directors, exposure from Cloud computing and exposure of Smart Devices as well as the Internet of Things (IoT).

Seemingly an order of magnitude greater than last year, *Forbes* identified 60 cyber security predictions for 2018. For example, IoT vulnerabilities in critical infrastructures are growing and the impact of breaches more dangerous. Adversaries are growing in sophistication and capabilities. Moreover, attacks will increase as well as become more weaponized, i.e. the US November 2018 election.

Finally, the global regulatory framework remains murky. With no clear leadership from the United States, the European Union will begin enforcement of the General Data Protection Regulation (GDPR) on May 25, 2018. Likely, a patchwork of regulations will emerge.

Certainly, enterprises need to adhere to the regulations of the locales in which they operate. However, a case can be made that the technology is outpacing governments worldwide.

Firms need to be proactive and exceed regulatory requirements to keep up with the bad guys. The business and technical models described herein are aligned with regulatory authorities but not dependent on them.

It's All About the Internet of Things

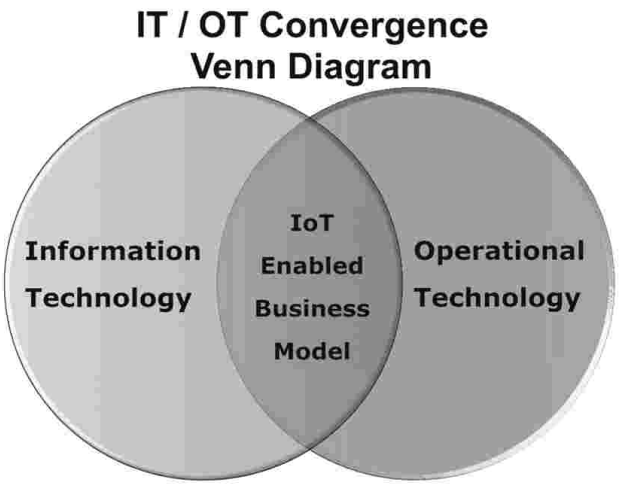
The Internet of Things is broadly defined. As with other IT buzzwords of their day, the specific meaning is in the eye of the beholder. Generally, the term refers to decision support data obtained from sensors or other sources and transmitted across one or more networks.

The decision maker can be either machine, human or a combination of both. Increasingly, this capability is the hallmark of Operational Excellence in High Reliability Organizations.

For asset intensive enterprises such as the energy sector, the convergence of Information Technology and Operational Technology(IT/OT) has the benefit of integrating process workflows with associated information flow. Expanded from Accenture there are five key steps to obtain this convergence:

- The firm must have an **Integration Strategy**;
- An appropriate **Governance Structure** must be put in place;
- **Change Management** throughout the entire enterprise is mandatory;
- Robust **Cybersecurity** is fundamental across all design and operations;
- The new business and technical models must be **Inclusive** across the organizational ecosystem.

It is tempting to view the convergence of two technologies strictly from the perspective of engineering and field operations. However, this type of focus has not been successful with previous IT initiatives if executives with Profit/Loss responsibility see IT as a cost and not aligned with business imperatives.



Source: The Rapid Response Institute

All five steps are more business process focused than technology driven. Certainly, information technology is pervasive; however, as with previous paradigm shifts, technologies are the enablers and not the ultimate drivers of change.

Without an identified integration strategy with *sustained* support from the chief executive officer, major organizational transformation ALWAYS fail. This is not something that can be delegated to an

executive sponsor (typically not the CEO) and expect that historic forces will not prevail.

Once the strategy has been decided, a governance structure must be put in place. This is a subject of a great deal of confusion in the modern enterprise.

Most are aware of the enterprise governance model with its primary focus on financial transparency. Likewise, typically large organizations have standing IT governance whose requirements are to assure alignment with the business model and the development of a technical architecture. Less understood is the role of governance in operations. Prior to the *Deepwater Horizon* incident in 2010, many saw operations from a field and engineering perspective. Supply chain management processes controlled contractors. The concept of an *ecosystem* was rudimentary at best for most.

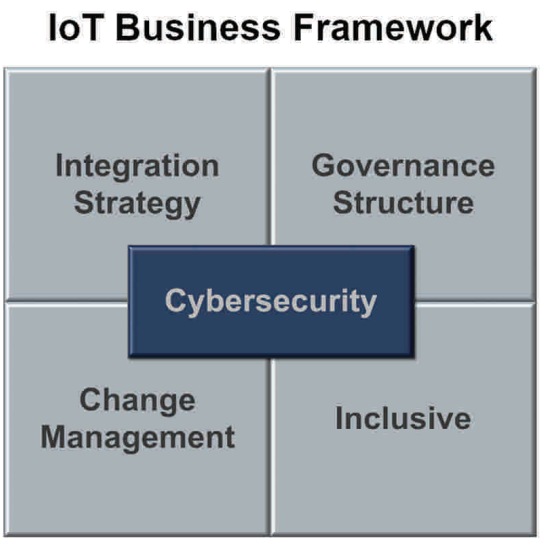
Moreover, once the sector began to implement the digital oilfield business model enabled by enterprise level Operations Management Systems (including thenew demands of the US and other regulatory bodies for transparency), things began to change. If this is the way 'we run the business,' the governance model must reflect this new paradigm.

Business Case

Robust Cybersecurity is fundamental across all design and operations. This statement explicitly states that organizations must make cybersecurity endemic across their ecosystem. It must become part of the culture, much like the Safety Culture is now who we are and how we do business.

Think of cybersecurity as the glue that holds the business framework together. In this sense, it is more than simply enabling technology. It is the policy, processes and protocols necessary to assure the enterprise that a robust cybersecurity program is in place.

Most integrated oil and gas enterprises are composed of at least three segments; upstream, midstream and downstream. Additionally, by some accounts, up to 90 percent of field personnel are contractors and their subcontractors and other non-operator employees.



The technological landscape also varies greatly as well. For example, upstream field operations maybe composed of legacy SCADA (circa 1980s) as well as the latest smart devices. Networks maybe a combination of legacy hard wired to the latest wireless meshes. Finally, supplier capabilities will vary widely too.

How can management be assured that their cyber risk mitigation strategy is effective? The following hypothetical discussion addresses the technological hybrid organization as mentioned. The landscape is complex and typical of the current state of the real world.

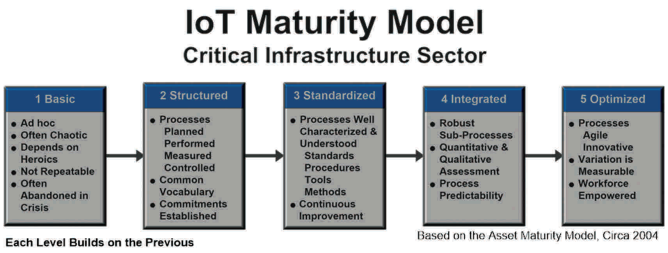
Using the IoT Business Framework model put forth above, the five steps are expanded herein. It is necessarily high-level; however, these basics can be built upon into an implementation plan.

Integration Strategy

Any new initiative should be well grounded and aligned with the business objectives. This pundit and others have made this case for decades. Yet, many still fail at this crucial step.

Begin with the first question. What is the organization's business model and why would an IoT initiative enhance that strategy? While this sounds simple, articulating the answer has proven to be illusive for many organizations.

It can be useful to use a maturity model when assessing the organization's readiness for new technologies. As shown in the following figure, our circa 2004 Asset Maturity Model (AMM) was put forth when the early digital oilfield initiatives were in their infancy. At the time research suggested that typical IT driven capability maturity models did not adequately consider the wide variability inherent to field operations.



For example, land operations in west Texas are very different from offshore Angola. A one size fits all approach may not be the best for such diverse operational requirements.

It is also tempting for management to set unrealistic expectations. An organization effectively at Level 2 cannot expect to launch a single initiative to attain and sustain Level 4 or 5. This process should not be viewed as linear. Step level changes are more exponential than that.

Moreover, there are costs to be borne and the economic value proposition needs to be well understood. Costs are not strictly financial either. A major commitment will be required to transform an organization into this new business model.

A candid assessment of the so-called "As Is" situation is imperative and management and the board of directors must be candid about

the business model. “To be” can never have an effective project plan if the starting point is incorrectly identified.

Management should clearly understand that nothing in this section or the article suggests that the organizations gets a pass on cybersecurity if the level of maturity is low. Paraphrasing, *we have to get it right every day and the terrorists only have to get it right once*. This needs to be the enterprise’s mantra!

Cyber-attacks are terrorist events. These criminals seek to destroy oil and gas processes and kill human beings. This point cannot be overstated.

Governance Structure

Effective governance can only follow the frank development of strategy, its risks and implementation plan. Governance is also one of the least understood issues of the modern enterprise.

If ‘this is the way we do business,’ then the enterprise governance and risk mitigation models must incorporate IoT and associated cyber exposures. This is now a board of directors issue, no less than financial transparency, i.e. Sarbanes Oxley.

When an item, process, technology or other ‘thing’ comes on to the governance radar, it cannot be delegated! The CEO cannot blame the CFO if accounting irregularities are uncovered. Nor can evidence of employee theft be solely the fault of Human Resources.

Governance lays down the ethical model to be followed with clear protocols. If it does not, there is a flaw that exposes shareholder value. Such faults must be identified and corrected.

Once the strategy has been identified, governance is the MOST important oversight of the digitalization process and the expected cybersecurity exposure. Those charged with governance (the board and C level individuals) must assure that appropriate, knowledgeable individuals with access to tools that protect the firm are in place.

This is no different than the management tools required to assure financial corruption and fraud does not occur. Again, fraud protection is not dependent on where a firm is on the maturity model. Cybersecurity these days is at least, if not more important, due to the gravity of failure.

On March 19, 2018 Facebook’s common stock closed down almost seven percent. The news reports suggest there may be several reasons for this market sell off. However, it appears that misuse of data may be one of the main culprits. As this article went press, this issue was still unfolding. Governance matters – a lot!

Change Management

Individuals resist change – a long-standing mantra! This pundit accepts this premise based on the fact that we are all still using rotary dial landline telephones – NOT! Billions of smart phones litter the globe. By some account there are more of these devices than there are people. Individuals respond positively to change when he or she sees value for themselves. Saving the company money, *et al.* is ok and all should be part of any corporate culture.

However, real value is derived when humans go the extra mile. If they have the “What’s in it for me mentality” (which we all do) then change is much easier. Will difficult questions be asked? Yes of course, but management needs to have the answers.

Technological and social changes are exploding. All of us must deal with this real politic. Putting change management processes in place is a management imperative.

Cybersecurity

After many highly publicized breaches including sophisticated government agencies (national defense entities of several countries as well) this remains a major concern. A cat and mouse game between organizations and its adversaries continues and as mentioned is accelerating.

High Cyber Situational Awareness is no longer a luxury. Every organization must have this mindset at its core and not just in the IT department.

Much of cybersecurity discussions focus on maleficence by bad actors. There is another culprit. Industrial espionage is not new and one can surmise that these actors also use cyber weapons to either learn secrets or disable competitors.

Realistic business and technical models need to be put in place. Robust software and expertise is available and ALL firms must take advantage of the current state of the art. Placing a company wager in this space may border on *gross negligence*.

The old phrase, ‘we are what we eat’ applies to IT systems as well. As noted, most organizations are a hybrid of several generations of information management and dependent on supply chain partners that may be even more diverse.

There is no scenario where current IoT technology can be deployed globally. Even if cost was not an issue, by the time the deployment was finished, today’s technology would most likely be obsolete.

By default, enterprises must deal with their technology legacy which may include devices and even systems that were never designed to deal with today’s threats. These systems create vulnerabilities that must be defended.

Fortunately, the cybersecurity sector has responded with tools that enabled legacy systems to be retrofitted to meet or exceed today’s cybersecurity protocols. Enterprises are well advised to evaluate these tools.

This also suggests that the chief security officer (CSO) have direct unfettered access to the board committees tasked with assuring the firm is cyber secure. This does not mean that the CSO and his or her team “go around” management but simply speak with a clear unfettered voice not unlike the CFO does regarding risk management and financial transparency today.

Inclusive

As noted, any firm in the energy sector depends on a number of other firms, outsourcing, engineering and construction, contractors, consultants and others. Don't forget the auditor and accounting firms as well.

Source: IoT with ROI

It is critical that the cybersecurity program encompass this ecosystem as well. Even the smallest exposure of the chain can expose the organization to a serious risk.

Historically, the corporate IT "firewall" has provided some protection from supply chain enabled errors or maleficence. These static systems may not be applicable going forward in a world of billions of sensors. A redefinition of this term and its management is in order.

Emerging Landscape

The technologic juggernaut marches on. Smart devices are everywhere and management tools available proliferate. This is a dynamic environment and one that must be monitored closely.

Various industry and horizontal task forces and working groups exist. One cannot join them all but selectively engaging relevant actions can be of high value.

Many argue that the rate of change today is as high as it has ever been and by an order of magnitude. Organizations are faced with exploding technologies such as Big Data Analytics, Artificial Intelligence and Edge Computing (applications, data, and services away from centralized nodes to the logical extremes of a network) to name few.

Other issues include the shortage of skilled personnel. This extends beyond cybersecurity experts and includes knowledgeable individuals to manage IoT applications and networks.

The management processes of digitalization are still unfolding. However, the sector has managed significant and rapid change before, i.e., commodity price point fluctuations. There is no reason to fear this new reality.

Implementation Plan

No firm, much less individuals or teams can know everything in the cybersecurity space. Events can overtake even the most sophisticated. The key is to be an informed and knowledgeable buyer of these goods and services. Moreover, good project delivery is critical and the development of strategy, governance model and the other three steps will reduce risk of failure as well as decrease the likelihood of a successful attack.

Effectively, this is the High Reliability Organization's implementation of a cybersecurity program. Resiliency after an attack is critical. Most experts agree that a cyber-attack is not 'Might' happen but is only 'When'. Resiliency is key to any risk mitigation strategy.

It is a challenge to address such a complex and important issue in these short pages. Readers may find the United States National Institute of Standards and Technology recent draft, "The Cybersecurity Framework" (available on line) an interesting read.

For example, eight Use Cases are provided that may have applicability to the global energy sector. These include:

1. Integrate Enterprise and Cybersecurity Risk Management
2. Manage Cybersecurity Requirements
3. Integrate and Align Cybersecurity and Acquisition Processes
4. Evaluate Organizational Cybersecurity
5. Manage the Cybersecurity Program
6. Maintain a Comprehensive Understanding of Cybersecurity Risk
7. Report Cybersecurity Risks
8. Inform the Tailoring Process

Finally, their Cybersecurity Risk Management Framework is shown in the following figure. It may provide a good starting point for many organizations and is freely available.

Source: NIST Cybersecurity Risk Management Framework

Final Thoughts

Every organization, public, private and anywhere in the world where employees, contractors or smart devices 'logon' to a public or private network are exposed to cyber criminals. Their intent can be monetary or perhaps more important the destruction of global critical infrastructures.

In either case, cybersecurity is a board of directors concern that cannot be delegated. Cybersecurity is one of the most important issues organizations of all sizes face.

About the Author

Dr. Scott M. Shemwell, sshemwell@theRRInstitute.com, Managing Director of The Rapid Response Institute 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 had been directly involved in over $5 billion of acquisitions 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 global energy and heavy industry sectors. www.theRRinstitute.com