Case Study: Trusted Communications in the Upstream Petroleum Industry

Talisman Energy Implements Wellsite Information Solution Using Trusted Communications

Written by Joel Tennison, Malibu Engineering & Software Ltd.

In collaboration with:

C.M. (Mo) Crous, Manager of Exploration Technology (Retired), Talisman Energy Inc.

John T. Ramsay, Q.C. Gowling, Lafleur Henderson LLP

Mike Neudoerffer, NON-ELEPHANT Encryption Systems Inc. (NE2)

Barbara McDonald, Malibu Engineering & Software Ltd.

Table of Contents

Executive Summary

> *There are no low-tech businesses. There are only low-tech companies that haven't applied technology to make their businesses more productive.*
>
> —Michael Porter, Harvard Business School

One of the material emerging challenges for the global petroleum industry is the growing need to ensure the secrecy, integrity and authenticity of its electronic data. On one hand, information technologies of various forms and sorts have failed to fully live up to their promise to add value to a corporation by increasing productivity, reducing expenses and streamlining business processes. On the other hand, the potential is evident for knowledge management technology to improve the efficiency and decision making capability within a firm. The greater the role that information plays within any company, the greater the need to carefully manage that information and make intelligent decisions about the technology that is trusted to ensure the secrecy, integrity and authenticity of all the information involved.

The purpose of this paper is two-fold. First, it examines the general challenges of information security and knowledge management facing the petroleum industry. Secondly, it provides a contextual example of these issues by describing a Trusted Communications pilot that was implemented for the geology department of Talisman Energy Inc. ("Talisman"), a major independent international exploration and production company.

The Beginnings of Trusted Communications

With the support of the Petroleum Technology Association of Canada ("PTAC"), and law firm Gowlings Lafleur Henderson LLP ("Gowlings"), a series of producers, technology companies and knowledge experts delved into thinking about an industry-driven solution for Trusted Communications. As a result of many discussions of the PTAC Trusted Communications workgroup, it was determined that the best way to prove up the concept of Trusted Communications, both from a technical as well as a business perspective, was to conduct an industry pilot. Thereafter, a smaller group of companies, led by Talisman, collaborated on making Trusted Communications a reality for Talisman's wellsite geology operations. A steering committee (the "Pilot Workgroup"), chaired by Mo Crous, Manager of Exploration Technology for Talisman, with representatives from Gowlings, NON-ELEPHANT Encryption Systems Inc. ("NE2") and Malibu Engineering & Software Ltd. ("Malibu"), was formed to initiate and oversee the pilot.

Principles of Trusted Communications

Trusted Communications is based on the premise that data is a corporate asset. It follows, as a result of this view, that data needs purposeful and deliberate stewardship on the part of the company that owns the data.

Trusted Communications can be described as a standard business operating environment whereby all information that a business needs to capture, relay, review, analyze and manage on an ongoing basis satisfies the following conditions:

- It is freely available to those entitled;
- It is secret to everyone else;
- The partners who exchange data are authenticated and validated parties;
- There is assured integrity as to origin, accuracy and currency;
- It is legally enforceable.

Validating Trusted Communications in a Wellsite Pilot

With the assistance of John Ramsay of Gowlings, Mo Crous of Talisman engaged two technology service providers, NE2 and Malibu, to develop a solution that would serve a current business requirement and could be used to prove the business value and technical merit of Trusted Communications. NE2 provided the encryption algorithm in order to establish a Trusted Communications environment during transmission and Malibu's Wellcore knowledge management solution handled the input, transfer and ongoing management and reporting of wellsite geology information.

The Business Case for Trusted Communications

One challenge with technology investments is measuring the business impact and value. For Talisman, the Trusted Communications pilot produced a series of benefits for the corporation, including:

- The implicit assurance that the data received is correct, secret when necessary and that it was sent from the correct person in the field and then delivered to the right people in the office and partners outside the company. Time savings were also realized by eliminating the need to confirm and reconfirm the validity of the data, and by the automatic distribution of the information.
- More transparent business processes that reduce the typical corporate "information is power" syndrome. All those who need to know information have access to it and this openness drives efficiency and encourages employee accountability and associated rapid response times.
- Higher quality and rate of knowledge transfer. A secure knowledge management solution ensures that business processes are explicit rather than tacit; there is less of a need to rely on prior social context(s) to interpret and understand information. The more standardized and structured the information is, the greater the ability for people to move between projects and teams with little difficulty and minimal knowledge loss.
- The ability to query and use current and historical geological information. A secure knowledge management solution incorporates business processes into the software and provides the ability for staff to customize data views, produce ad-hoc reports, make comparisons, drive workflow and measure progress over time.

Pilot Results and Next Steps

Talisman successfully piloted the Malibu-NE2 solution this summer, 2002. Geological information was successfully and securely captured, transmitted, analyzed and distributed internally and externally by Talisman. Effective December 2002, Talisman is going forward with the Malibu-NE2 Trusted Communications solution within their wellsite geology operations for the next winter drilling season, a period of peak drilling activity.

An area of further focus would be the encryption of data and information while resident on the local hard drives of laptops, desktops and servers. Once this is in place, and augmented by the use of username, password and SecurID or similar device, then the full Trusted Communications model will be in place.

Introduction

Knowledge Management in the Petroleum Industry

For any organization, no matter the size or industry, knowledge is critical. This is especially true when considering that knowledge is, by definition, "the sum or range of what has been perceived, discovered, or learned." In the last few years, with the advent of the post-dotcom world, there has been much talk of "knowledge workers", the "knowledge economy" and all sorts of other things relating to the nebulous term "knowledge". Nonetheless, progress of any kind cannot occur without the application of knowledge. Consider how crucial it is for an organization to be able to manage its own collective knowledge. In the private sector, the firms that best capture and leverage their knowledge generally dominate their field. Knowledge forms the basis for making wise decisions.

In the petroleum industry, as in other verticals, there is a growing importance being placed on the ability to manage knowledge. Exploration and production (E&P) companies of all shapes and sizes are increasingly being forced to come to grips with how they are managing their business information. Many are looking to leverage the potential of information technologies to improve their ability to increase production. Petroleum producing and servicing companies have a need to capture all sorts of information and organize it in a meaningful way that incorporates their business processes, enhancing the decision-making ability of management.

> *Technology is changing the way in which oil and natural gas companies do business. Primarily the change relates to instant availability of information, transparency of data, and the speed at which communications take place. Many of the changes that have taken place in the past were driven by major events or inventions, most of which took many years to permeate the business fabric of the nation and the world. Information technology and the communication revolution it creates have taken the world of business by storm in a very global way. National boundaries, which used to provide some stability for business activities, no longer are a limitation. Information, which used to be relatively easy to protect physically, is potentially vulnerable to an individual who has access to a computer and a way into the global information network.*
>
> - Securing Oil and Natural Gas Infrastructure in the New Economy (National Petroleum Council. June, 2001)

In addition to storing historical data over time and being able to manipulate it in ways that add value to decision making, there is also the need for the information in question to remain private and inaccessible to outside parties. Information security and knowledge management are key concepts that require consideration; they are also both part of an overall Trusted Communications environment.

The Pilot Approach

One way E&P companies are attempting to address the challenge of gauging the business value of technology investments is through the use of pilots; projects that are deliberately small in scope and that can validate or negate early thinking and hypotheses about the benefit(s) of a particular technology solution and corresponding capital investment.

This paper describes a pilot that Talisman, a Calgary-based global exploration and production company, undertook with the help of some knowledge experts, service providers and software companies. Specifically, the pilot was in the area of Trusted Communications, and it dealt exclusively with the wellsite geology operations. In addition to the need for information to be successfully captured in the field, transmitted to the office and partners and analyzed, the data had to remain secure and private.

Principles of Trusted Communications

The notion of Trusted Communications is based on the premise that a company's data is a valuable corporate asset. Trusted Communications can be described as a standard business operating environment whereby all information that a business needs to capture, relay, review and manage on an ongoing basis satisfies the following conditions:

Fundamental Security Requirements

Requirement	Explanation
Access Control	Determines who may have access to information within a system. Information is freely available to those entitled.
Authentication	Verifies the identity of communicating parties. The partners who exchange data are authenticated and validated parties.
Confidentiality, Privacy and Secrecy	Protects all information, including sensitive information from being viewed indiscriminately. The information is secret to everyone else.
Non-Repudiation	Inability to disavow a transaction; the transaction is legally enforceable.
Integrity	Electronic record has not been altered; there is assured integrity as to origin, accuracy and that it is current.

The Need for Trusted Communications

The Cost of Information Interception

The global petroleum industry consists of literally thousands of E&P companies who endeavor to grow by differentiating themselves from their peers, based mainly on their ability to find and produce oil and gas cost effectively and increase their reserves. Whether increasing production through the drill bit (exploration and development) or through strategic asset acquisition (exploitation), there is considerable time, effort and analysis required on the part of an upstream E&P company. Often, part of the analysis involves the transmission of detailed technical information between the field, the office and partners.

The PTAC Trusted Communications Workgroup

The Petroleum Technology Association of Canada (PTAC) is a not-for-profit association that facilitates collaborative research and technology development in the petroleum industry. PTAC acts as a mechanism that facilitates collaboration on research and development to the benefit of those involved. In this regard, PTAC facilitates a series of industry workgroups; these organizations consist of representatives from E&P companies, technology and service providers, data vendors and leading knowledge experts.

From October 2001 to June 2002, the PTAC Trusted Communications workgroup got together to discuss and develop a Trusted Communications solution for the oil and gas industry.

Concurrently with the PTAC Trusted Communications workgroup, PTAC and Gowlings convened a working group of a number of solution providers to the petroleum industry to encourage formal and informal collaboration amongst them. Each member agreed to make their products interoperable when economic conditions were appropriate, with the expectation that compatible "best of breed" products would be more competitive if NE2 and Malibu were active participants in the workgroup.

John Ramsay of Gowlings brought Talisman, NE2 and Malibu together to encourage an industry pilot. By conducting a pilot, Talisman believed it could prove up the validity of the Malibu-NE2 solution.

The Talisman-Malibu-NE2 Pilot

Talisman purposely limited the scope of the pilot; the philosophy was to "walk before you run". By conducting a pilot, Talisman believed it could verify the validity of the combined Malibu-NE2 solution. This mitigated the potential initial outlay of capital; it also allowed for the solution to be optimized prior to implementation. By focusing only on wellsite geological information, the pilot could prove up a concept that had broader applicability within Talisman while only minimally impacting employees not directly working on the pilot.

The pilot had four main phases:

- Establishing the guiding principles;
- Testing and adaptation of Malibu's Wellcore Geological module to meet Talisman's requirements;
- Integrating and testing NE2's security module, the NE2:GRID product with Wellcore's Communications module, for high speed communications (i.e. high speed satellite dial-up and Ethernet connections);
- Integrating and testing NE2's security module, the NE2:GRID product with Wellcore's Communications module, for low-speed communications (i.e. regular dial-up, low bandwidth cellular communications).

Companies, Roles and Products

Company	Roles and/or Product
Talisman Energy	Talisman provided the overall vision and business driver for the wellsite geology pilot. Mo Crous, Manager of Exploration Technology for Talisman, was the original sponsor of the Malibu-NE2 solution. Mo Crous conceived of the original vision and was an active participant in the PTAC-Gowlings Trusted Communications workgroup.
Gowling Lafleur Henderson LLP	Gowlings sponsored the original PTAC meetings of the Trusted Communications group. John Ramsay, a partner with Gowlings, facilitated the initial meeting of the pilot companies, Talisman, NE2 and Malibu. Mr. Ramsay brought forth the very critical legal and liability perspective to the group and the pilot. His role as a neutral third party was essential in being able to ask the difficult questions during the pilot.
NON-ELEPHANT Encryption Systems Inc. (NE2)	NE2 provided the encryption component for the pilot. Specifically, it was the NE2:GRID product that provided the secret, dynamic key exchange over both high- and low-speed communication required for Trusted Communications. NE2:GRID also provides a packet encryption solution, whereby each individual packet sent and received over the secure communications channel is encrypted.
Malibu Engineering & Software Ltd.	Malibu's Wellcore geological module captured the daily well site geological information, transmitted it to the Calgary office and then distributed this information to designated recipients within Talisman and its partners. Wellcore was installed on field laptops as well as on an office server. The Wellcore database archived all the field information received making it available to Talisman geology office personnel and management. These individuals were then able to access, retrieve, report on and analyze the field information.

For more information on the organizations involved in the pilot, please see Appendix I.

Pilot Developed for Tight Hole Situations

Upstream E&P companies compete based on their ability to increase reserves while producing oil and gas cost effectively. If indeed a firm thinks they differentiate themselves from the competition based on their ability to do so, then they obviously value any and all information related to this ability. Therefore, without an environment where Trusted Communications exists, the potential competitive advantage that is derived from superior knowledge and analysis capabilities is at risk of being lost.

One obvious place where Trusted Communications is critical is in tight hole situations. Given the history of scouts in the oil and gas industry, there is a need to ensure information cannot be intercepted; that it remains secret. This point is even more obviously clear when one considers the potential risk—and associated financial cost of a missed opportunity—of having critical information about a potential play compromised. Consider the following example:

Lost Opportunity Scenario	
Potential Total Reserves	25 bcf
Total Capital Expenditure Budget	$71 million
Net Present Value of Total Reserve Income	$50 million
Well cost (per well)	$1 million
Number of Wells	10
Total land cost	$2 million
This represents a lost opportunity cost of $50 million.	

Additional considerations in the case above:

- Larger projects tend to have more people involved; the more people involved, the greater the chance for information to be compromised. Also, the larger the project, the greater the likelihood of an attempted unauthorized theft of information due to the greater potential value of the information.
- Longer projects
    - Those projects with multiple wells in a larger area tend to have more parties involved, and higher staff turnover rates. Therefore, the need for security is heightened with projects that are longer in duration.
    - Projects with deep wells and multiple wells on single properties will be transmitting tour sheets and other secret data from the same location over a long period of time. As a result, the probability of scouts being able to set up successful listening posts increases significantly.

Trusted Communications Drives Workflow Improvements

Another area to consider in thinking about the business case for an E&P company establishing Trusted Communications is in the area of workflow improvement, within a company and with partners. Because of the scale of operations and the ability for a company that is drilling a well to spend a large amount of capital in a short period of time, there is often a need for employees in the field to confirm information and instructions with people in the office and vice versa.

The process of confirming—usually by phone—what was in an email, or on a fax report is cumbersome; it adds no value. Trusted Communications will ensure that the electronic data did indeed originate from the original party and was received fully and untampered by the receiving end and will lessen the need to re-check and re-confirm all this data and instruction. Rechecking increases the risk of loss of secrecy.

The Trusted Communications Pilot

Drawing on the work done by the PTAC Trusted Communications workgroup, the Pilot workgroup developed the following wish list for fully-secure Trusted Communications:

- Secrecy of data in transmission;
- Secrecy of data in storage;
- Transparency (no user interaction should be required as the Trusted Communications is "always on" and invisible to the user);
- Ease of use;
- No additional hardware investment required;
- Cost effective solution;
- Authentication to a specific computer device;
- Authentication to a specific person.

In addition to the objectives above, the Talisman geological department wanted to replace RDS, the existing geological information management solution. In its place, the group wanted to implement a solution that integrated business processes, provided customized views of the data and incorporated the use of existing pervasive file formats.

Unfortunately with present technology, some of the goals from the wish list were incompatible. The level of trust chosen involves a balance between security and convenience. The higher the level of security desired, the less convenient is the solution. The less convenient and more difficult to implement, the more likely the implementation will fail (a known result) or will be defeated by individuals under pressure to get the job done (often an unknown result).

To better understand how to deal with this balancing act, the Pilot workgroup looked at current practices, but resolved to adopt a mindset for proceeding with testing rather than planning for perfection, with the risk of never accomplishing anything substantial.

Pilot Results and Next Steps

The pilot results have been successful. Geological information was successfully and securely captured, transmitted, analyzed and distributed internally and externally by Talisman. The technical teams from NE2 and Malibu have collaborated to produce a robust, secure knowledge management solution for Talisman Energy's wellsite geology operations. Final testing and quality assurance processes are occurring at the time of the publishing of this

paper. Effective December 2002, Talisman is going forward with the Trusted Communications solution in their wellsite geology operations for the winter drilling season.

Examining Current Practices

In terms of discussing a solution, the Trusted Communications workgroup felt it was important to understand a) how things were currently being done and b) the associated challenges and risks with the existing technology and business processes. The following is a list of the mechanisms and associated business impacts and/or risks that are currently used for information security by most oil and gas firms:

Existing Mechanism	Business Impact and/or Risk
Username and password access to computers, files and some applications	Standard protection; open to both social hacking and brute force attacks.
Password-protected, zipped files	Requires personal end-user judgment to know which files should be protected.
Files exist in multiple versions and reside in more than a single location	Results in data re-entry, lack of data integrity. Risks the performance of the company if decisions are made on incorrect information.
SecurID, SmartCards and Digital Certificates	Authentication to a person is expensive and often complicated to administer.
Digital Signatures	An electronic signature is irrefutable, unique, and virtually impossible to copy or transfer; they are, however, relatively expensive to administer.
Encryption—static or fixed keys	Static keys provide security only if they remain secret. Since the keys are not regenerated, once a fixed key is acquired, all information can be intercepted and decrypted by whoever has the key.
Encryption—dynamic keys	Dynamic keys offer greater information security, but are often costly to implement. Extensive management is required as dynamic key generation is often difficult to administer.

The challenges as a result of the means listed above are several. E&P companies often rely on nothing other than hope in terms of keeping information secure; this is the default position in the case where a company makes little or no concerted effort to implement an information security solution of any sort.

Cost Benefit Analysis for Trusted Communications

The Pilot workgroup assessed the risks involved using the following factors developed by the PTAC Trusted Communications workgroup:

- The cost of the proposed security versus the cost of not having security;
- How often a particular kind of security breach actually occurs;
- Whether a breach causes demonstrable harm;
- The dollar value of the damage caused by a particular kind of breach (example above);
- The non-monetary value of the damage:
    - What value does one assign to the unauthorized disclosure of personal information, corporate information, to the loss of customer, employee, investor or public confidence?
- Examine the potential for catastrophic harm with remote chances of occurring compared to potential for lesser harm with greater probability of occurring.

Legal Implications of Trusted Communications

The Pilot Working Group then examined the legal standards of care and for security that could be involved:

a) There was no statute or regulation that set any legal standards;

b) There was no known public policy that might demand a particular level of trust; the intended use did not involve highly sensitive data such as health records, personal data, data relating to children, etc.;

c) There was no risk of personal injury and death or material property damage as a result of information having been disclosed or incorrectly reported;

d) The anticipated loss was only economic loss, although that loss could be substantial;

e) There were no known contractual obligations. There is a concern that some relevant contracts could have requirements to "ensure" secrecy, or "take all necessary measures to maintain secrecy", or simply "maintain secrecy" all of which could require the highest level of trust no matter the inconvenience. There is a suspicion that there is a dysfunction between the terms of these contracts and actual practice, but it was considered more appropriate to get the contracts into line with reality, rather than adopt practices to legal contractual standards that may have been adopted without discernment.

The Pilot workgroup endeavored to strike a balance where the maximum trust level could be obtained with the least cost and minimal inconvenience.

Organizational Challenges

In addition to the challenges that are more technical in nature, there are also organizational challenges when a firm explores the possibility of introducing a Trusted Communications environment. Some organizational challenges that were considered:

- "Information is Power" syndrome;
    - Different organizations, departments and teams tend to protect their relative territory by controlling the access to and flow of information. A more transparent, organization-wide knowledge management system, along with the appropriate business processes, would mean that workflow is streamlined. Knowledge of what work is being done by whom would be freely available to those people who are deemed appropriate—those with access. Knowing that a particular group's actions will be scrutinized and fully available to other teams and leaders within the corporation, each group will ensure they are delivering on commitments and doing the best they can to push work forward—to expedite the steps/processes that are required in order for the company to do its core work.
- When things go wrong, people clam up;
    - A document management/knowledge management solution ensures accountability throughout the organization. This accountability also means that companies can identify and address problems early on in the process and limit additional business cost as a result of otherwise ignoring what has occurred. For example, consider a wellsite blow-out that is very costly to an E&P company; having secure knowledge management system ensures that the issues are known to both field and office personnel in a timely manner, limiting liability.
    - A wider range of experts can be allowed, even charged, to scrutinize the data to find the subtle key to solving the problem.
- Difficulty conveying importance of having Trusted Communications;
    - With no formal system in place, you default to the judgment of individuals. Some of the time, there are lower-level workers who lack perspective of the importance of and the knowledge of the use by others in the organization. They send around information freely and unprotected, innocent to the potential damage in case of a leak.
- Building the business case is a challenge;
    - This is especially the case when you are paying a certain sum of money in order to *not* be subject to something. In a sense, strictly looking at an information security solution, it is analogous to purchasing insurance.
    - Despite the weaknesses in the current system, the oil and gas industry is quite successful – "It ain't broke; don't fix it!"
- Impossible to capture intuition in information management systems;

- In many cases the clues to future success are very subtle, and hidden among large quantities of data. It is the wizened intuition of the experienced worker that picks up on it.

❖ Trust is absent, yet people have a tendency to put their faith in electronic information management systems even though the information may be incomplete, inaccurate and not current. Therefore management uses elaborate checks and balances to safeguard against future disasters.

❖ A broad variety of communication mechanisms are used to send and receive information, including satellite (dial-up or IP service), analog cellular and microwave.

The Future of Computing Infrastructure

The PTAC Trusted Communications workgroup wanted to ensure the relevancy and interoperability of any secure information management solution. To do so, they examined a number of the large forces driving the evolution of computing infrastructure, including:

❖ *Distributed computing*: Any computing that involves multiple computers remote from each other that each have a role in data storage and information processing. For E&P companies, this refers largely to the multiple sets of distributed data that need to be managed (i.e. regional databases managed by regional data stewards on servers right at their location rather than transmitted and assembled centrally);

❖ *Encryption Algorithms:* The mathematical algorithms used to scramble information. Symmetric encryption uses the same keys to encrypt and decrypt, whereas asymmetric encryption uses separate keys to encrypt and decrypt information. Great promise lies in encryption technology that generates identical keys locally, thereby eliminating the need ever to transmit the keys;

❖ *Intranet, extranet and Internet links*: The lines between these types of networks are blurring. Web-based applications and corporate portal environments are becoming prevalent in the industry; the end-user need not know or be concerned when the signals switch from one network to another;

❖ *Object-centric computing, XML, SOAP and Java*: Advances constantly occurring in software development languages, environments, processes and levels of interoperability, thereby eliminating hardware platform dependence and operating system dependence. Electronic commerce is increasingly important as oil and gas firms look to technology to maker closer, richer connections with their networks of customers and suppliers;

❖ *Graphic user interfaces, maps and pictures*: Map-based front-ends have become a familiar user interface, particularly in the areas of geology and geophysics; this familiar interface can be extended to all types of data: "A picture is worth a thousand words";

❖ *Customized and personalized software*: The ability for people to customize their own software working environment and workflows unique to their department and company is increasingly important. In addition, if a worker can be empowered by personalizing the interface and workflows, i.e. make them conform to his or her own

intellectual style, all obstacles will be removed from the mind-machine interface. Productivity will jump and "computer rage" and frustration will decrease;

- *Word, Excel, Access, Lotus, etc. file formats*: Because of the pervasiveness of these types of files, there is a need to accommodate these file formats and provide the capability to import and export to and from them freely and without end-user intervention.

Establishing Guiding Principles

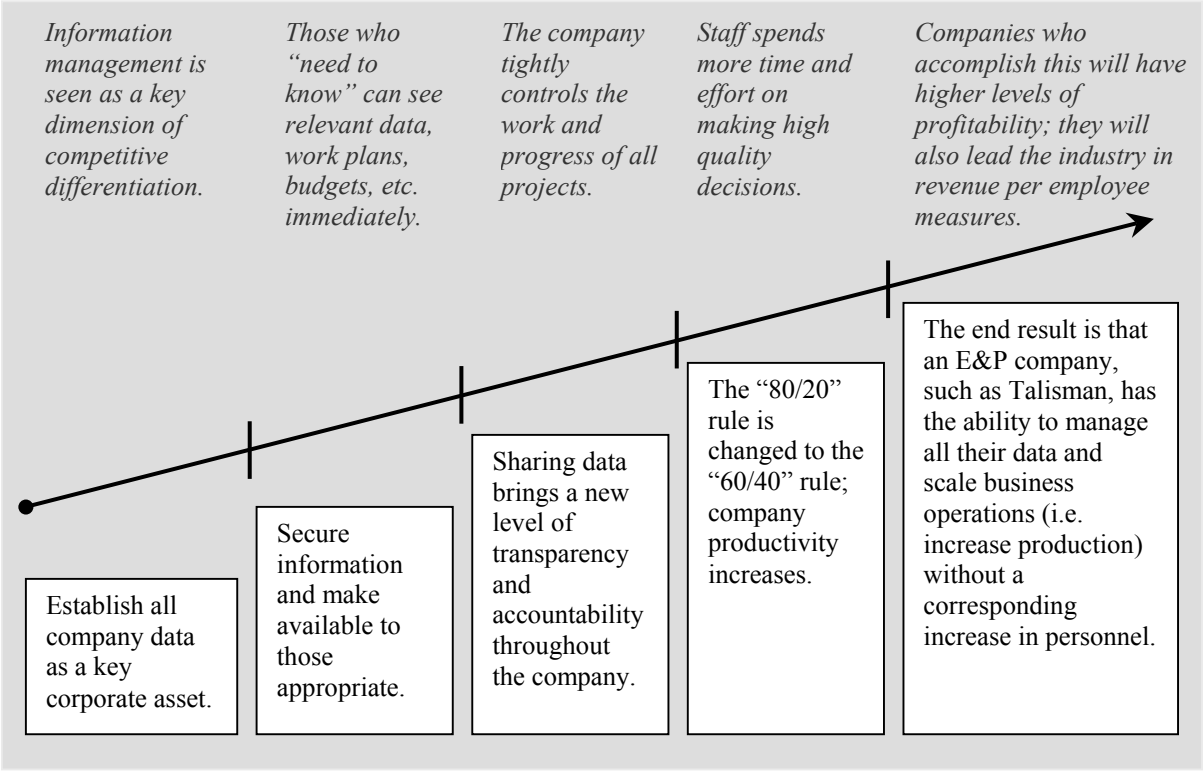
Given consideration of both the current means to secure data with an upstream E&P company (and the associated challenges/risks listed above) and the future of computing infrastructure, the Trusted Communications group defined some important guiding principles as follows:

- Data is regarded as a corporate asset;
- Data should be under the stewardship of one organizational unit or one person;
- Those most informed and involved employees should manage and control the data. The individuals who are fully dependent on data accuracy, timeliness and completeness are the stewards;
- Data should reside in only one database—only one copy shall exist;
- Links and/or rules of entitlement shall govern access to that one copy of the data, wherever it may reside, as part of distributed data sets;
- Standard business processes need to exist to enable people to learn about the characteristics of Trusted Communications. They don't have to know how to do it, but they need to know that there is no longer the need to validate or authenticate Trusted Communications;
- Transparency: Trusted Communications needs to be part automatically—and by default—of how employees do business without interfering or causing delays; it should be invisible to the users;
- Trusted Communications needs to be used consistently and without exception. If Trusted Communications is not transparent, a company begins to rely on the subjective judgment of employees to determine whether information should be protected. The challenge is the sheer number of people who touch all the different pieces of data throughout the process – and unless they all make the "right" choices about encrypting documents/files, information, you have a risk. A weakness in one area may expose the entire system. Therefore, all-encompassing implementation is recommended, transparent to the end-user.

Benefits to Talisman

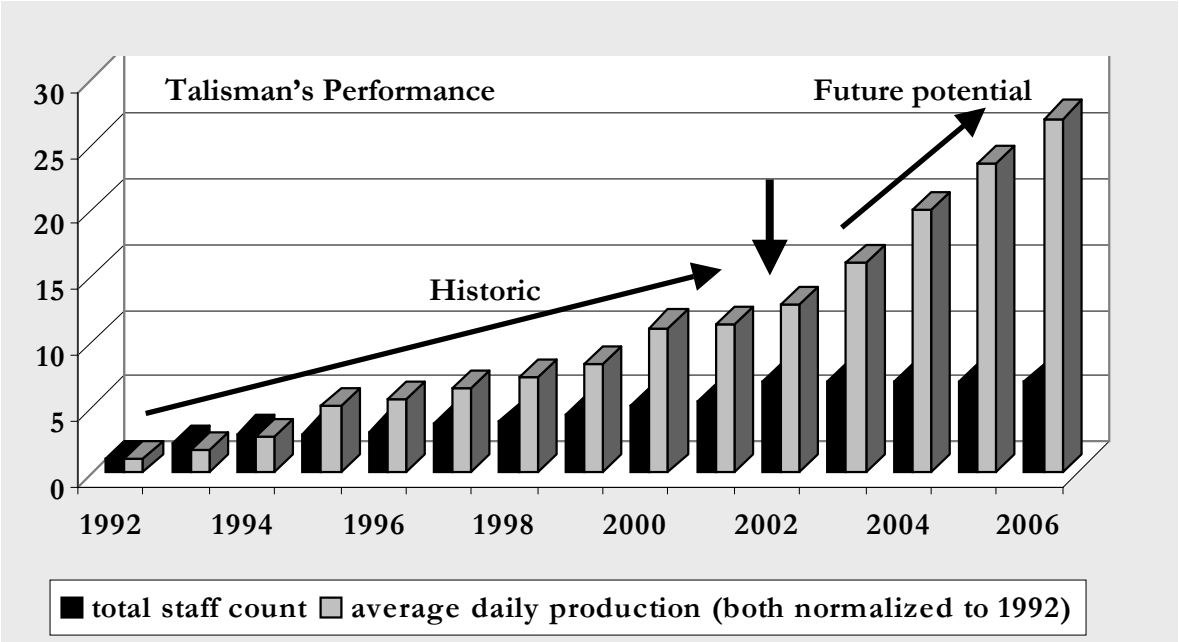
Mo Crous believes that adopting Trusted Communications throughout a corporation will improve efficiencies in daily operations. Consider the standard GG&E (Engineer, Geologist & Geophysicist) professional rule of thumb where 80% of time is spent on essential data gathering, authentication, validation and assimilation activities and 20% on value adding

decision support. Thinking in this 80/20 construct, Mo Crous believes that Trusted Communications can reduce all the double-checking and confirming figures, data and communications, so that the balance can shift from 80/20 to 60/40 – this means that productivity can increase by a factor of two by enabling employees to spend twice as much time on production-increasing activities.



What does it all mean?

What is the natural business hypothesis that results from the shift of peoples' time from non-value adding to value adding work? As the following graph displays: A company such as Talisman Energy would be capable of increasing the company's production level without the need to proportionally increase the number of personnel. In this sense, Trusted Communications, together with other initiatives to increase efficiency, while maintaining effectiveness, has the potential to impact key corporate and market indicators such as profitability, earnings per share and revenues per employee, among other measures.



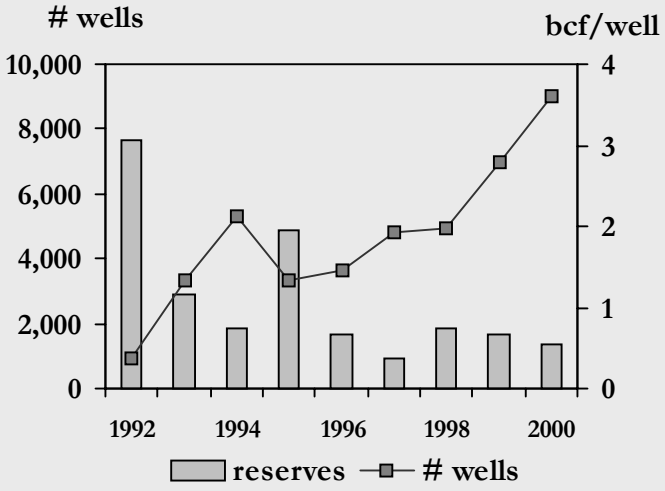
Consider also the table and graph below. E&P companies are increasingly faced with the reality of smaller and smaller pool sizes. As a result of the decreasing number of large pools being discovered by the industry (left hand table below,) and the larger number of wells each with decreasing reserves per well (right hand graph below,) the task is ever more difficult to maintain and increase overall production. The greater this is the case, the greater the need for E&P firms to increase efficiency, and the appeal of introducing Trusted Communications into their business practices.

World Giants

Decade	Number	Av Production/field (mboe/day)
pre-1950's	19	557
1950's	29	330
1960's	24	242
1970's	24	236
1980's	15	176
1990's	11	126

- Simmons & Company

Western Canada Gas Reserves per Well



- CAPP, 2001

Pilot Approach—Where can we start?

The Pilot workgroup determined at the outset of their discussions that the need for a technology solution of any sort would have to be driven from a business perspective. They agreed that any project to be undertaken to pilot Trusted Communications would need to add real business value. In order to realize value from Trusted Communications, they examined the various critical business functions within an E&P company and cross-referenced those with all the types of corporate communication that is required for ongoing operations.

In looking at one specific area, the ability to manage all the analysis and technical information within an exploration and production company, data about potential plays—wells that are being considered to be drilled—is some of the most important information that exists. For a competitor, even having a clue that a company is looking at a given area can risk losing an opportunity if that competitor takes according action to look into, acquire land and exploit.

The following chart, developed by the PTAC Trusted Communications workgroup, is the conceptual matrix the Pilot workgroup used to think about what information could be subjected to a Trusted Communications environment. In the case of the Malibu-NE2 pilot, Wellcore documents provided the format and interface into which wellsite geology information would be inputted.

		Critical Business Activity				
Critical Business Communications		Corporate Strategy	Acquisition & Divestiture	Production Operations	Finding & Development	Projects
	Action Plans				▨	
	Decision Support				▨	
	Business Activity					
	Transactions					
	Information				▨	
	Raw Data				▨	

▨ = Impact of the Talisman-Malibu-NE2 pilot

Preparing for the Pilot—Malibu's Creation of Talisman's Documents

For the 2002/03 drilling season, Talisman will have between 25 and 30 users in the field and between 20 and 30 users in the office. The pilot was an opportunity to "prove up" the Malibu-NE2 solution in a particular small yet key and ongoing area of operation.

As a result of Wellcore's flexibility, Malibu was able to incorporate electronic versions of all of the required Talisman Geological documents into the Wellcore solution. The types of information created or embedded into documents by Malibu included:

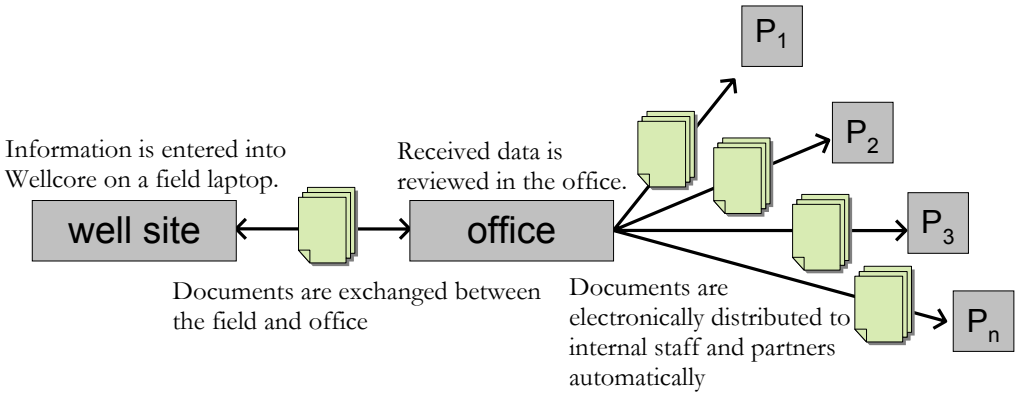
- Daily progress reports;
- Rock cuttings description (strip logs);
- Mud gas concentration;
- Drilling breaks, shows;
- Formation tops identified ("formations");
- Anticipated activities for next 24 hours;
- Recommendations for specific actions.

In addition to the specific documents listed, the Wellcore solution provided the functionality to embed files of any sort. Therefore, in addition to inputting information into the Wellcore forms, Talisman users have the option to attach files such as spreadsheets, images taken with a digital camera, text files and anything else. In this regard, the solution matched one of Talisman's original guiding principles around ensuring the company's employees can continue to work with major file types they are familiar with whenever appropriate.

For some screenshots of the documents that Malibu created for Talisman's geology group and of the NE2 key generation window, please refer to the Malibu web site at http://www.malibugroup.com/trustcom.html.

Automatic Partner Notification

One of the features of Wellcore is Automatic Partner Notification (APN). This functionality allows for documents of any sort to be automatically emailed out to specific people, internal or external to an organization. This feature is particularly relevant to field reporting and to the automated distribution of daily geological, construction, drilling, completions and reclamation reports. However, it applies equally to all Wellcore documents. In the Talisman-Malibu-NE2 pilot, Talisman set up Wellcore so that the daily wellsite geology information would be received in the office, converted to a standard HTML document and automatically emailed to a select group of individuals at partner companies.



NE2 :GRID

To ensure data integrity and secrecy, the pilot leveraged the NE2:GRID product to provide the following:

- The ability to generate truly random encryption keys on communicating digital devices—the keys are identical and created on each device without communicating any of the key data being exchanged. As a result, an outside intruder can view no key data, preventing key theft or attack.
- The capacity for transparently encrypting and decrypting real time data—there is no interaction required by an individual application or users of the application. In the case of this pilot, this means that Talisman field and office people do not have to interact at all or in any way with the information encryption process.
- "Tunable Secrecy": the ability to generate keys on demand. Talisman can specify how often keys are re-generated and therefore the level of secrecy. Tunable Secrecy allows for a higher level of security where a single transmission could have a number of encryption keys encrypting and decrypting it while it is being transmitted.

The impact for Talisman is that the NE2:GRID product delivers a highly secure encryption solution that is "always on" and one which requires no user intervention to employ or configure.

NE2-Malibu Collaboration

During the pilot, there was a need to ensure that the NE2 security solution was fully functional with Malibu's Wellcore Communication module. From April through August of 2002, the technical teams of Malibu and NE2 collaborated to produce a working solution for both high and low speed communication. This testing and quality assurance also involved soliciting input from key Talisman stakeholders to ensure that, once completed, the solution would be not only usable but also valuable to end-users.

The key challenge for the teams was to ensure a smooth process for the dynamic key generation within the communications process—in this regard, both NE2 and Malibu spent considerable time testing and analyzing the solution. This needed to be accomplished with a high level of reliability and with minimal impact on the speed of transmission. All of this also needed to be transparent to the end users; the transfer and use of data needed to occur without the users having to think about or do anything with it. These goals were accomplished.

Pilot Results

The initial pilot results have been successful. The technical teams from NE2 Encryption and Malibu have collaborated to produce a robust, secure knowledge management solution for Talisman's Geology business unit. Final testing and quality assurance processes are occurring at the time of the publishing of this paper.

Pilot Wish List Revisited

Let us review the wish list and see how the pilot did:

- Secrecy of Data in Transmission. Achieved in the office environment—NE2's algorithm has been verified by independent academic validation;
- Secrecy of Data in Storage. Not part of pilot and therefore yet to be undertaken as a further project;
- Transparency. Achieved;
- Ease of Use. Achieved;
- No Additional Hardware Investment Required. Achieved;
- Cost Effective Solution. Achieved;
- Authentication to a Specific Computer Terminal. Achieved (entity is correct); and
- Authentication to a Specific Person. Not Achieved, but rejected from priorities since achievement would require loss of other advantages including convenience.

In addition, the other mentioned Talisman requirements were also all achieved: RDS was replaced, the solution integrated business processes and provided customized views of data and incorporated the use of existing pervasive file formats.

Next Steps

Going forward, Talisman is planning to use the Malibu-NE2 solution as its Trusted Communications solution in the area of wellsite geology information for the upcoming winter drilling season. Approximately 25 field users and 25 office geologists will use the Malibu-NE2 solution to manage their work and improve the quality of decision making. Pending the results within the wellsite geology operations, Talisman will keenly assess the implementation of Trusted Communications in other areas within their organization.

Acknowledgements

Talisman Energy Inc.

Mo Crous, Manager, Exploration Technology (Retired.)
Keith Glenday, Team Leader, Wellsite Operations and Petrophysics
Glen Fullerton, Network Specialist
Kelvin White, IS Technical Architect

Gowling Lafleur Henderson LLP

John Ramsay, QC

Malibu Engineering and Software Ltd.

Barbara McDonald, Vice President, Business Development
Joel Tennison, Manager of Marketing

NON-ELEPHANT Encryption Systems Inc.

Mike Neudoerffer, Vice President, Business Development
James McRoberts, Vice President, Sales & Marketing

Petroleum Technology Alliance Canada (PTAC)

Eric Lloyd, President
Heather Traub, Technical Event Coordinator
Trusted Communications workgroup

Appendix I: Pilot Participants

Talisman Energy Inc. *(http://www.talisman-energy.com)*

Talisman Energy Inc. is one of the largest independent Canadian oil and gas producers with operations in Canada, the North Sea, Indonesia, Malaysia, Vietnam and Sudan. Talisman is also conducting exploration in Algeria, Trinidad, Colombia and the United States. Talisman has adopted the International Code of Ethics for Canadian Business and is committed to maintaining high standards of excellence in corporate citizenship and social responsibility wherever it does business. The Company's shares are listed on The Toronto Stock Exchange in Canada and the New York Stock Exchange in the United States under the symbol TLM.

Gowling Lafleur Henderson LLP *(http://www.gowlings.com)*

Gowling Lafleur Henderson LLP (Gowlings) is one of Canada's leading diversified business and technology law firms, with more than 100 years of success in employing specialized knowledge and vigorous thought to create practical legal solutions. Gowlings is at the leading edge in new fields such as technology and intellectual property, providing comprehensive legal solutions, in English and in French, to clients in Canada, the United States and overseas from offices in Montreal, Ottawa, Toronto, Hamilton, Waterloo Region, Calgary, Vancouver and Moscow. The firm also offers specific expertise concerning transactions in the United States, Mexico, Latin America, the Pacific Rim, Western Europe and the Commonwealth of Independent States.

NON-ELEPHANT Encryption Systems Inc. *(http://www.ne2encryption.com)*

NON-ELEPHANT Encryption Systems Inc. (NE2) is a security software development company based in Calgary, Alberta, Canada. NE2, established in 1999, develops powerful digital security software based on a radically new mathematical model that has resulted in a number of patent registrations. NE2's digital security products are securing various enterprise markets, including the oil and gas sector. These products insure secure real-time data transmissions and work invisibly over any network, including the Internet. NE2 is currently working to secure the 802.11b wireless protocol and future targets include securing PDAs and cell phones. NE2 strives to be innovative and continues to move digital security into a new era

Malibu Engineering and Software Ltd. *(http://www.malibugroup.com)*

Malibu is an innovative, client-centric software company that develops powerful cost control, knowledge management and productivity improvement solutions for the petroleum industry. With over 20 years of industry experience, Malibu has consistently produced innovative technology solutions for the exploration and production (E&P) and oilfield service markets. Wellcore, Malibu's flagship product, is a database solution that empowers petroleum companies to control costs and manage operations throughout the life cycle of their wells. Wellcore modules include Cost Control, Prospect Start-up (G&G), Construction, Drilling, Completions & Workovers, Regulatory, Abandonment & Reclamation, Scheduling and Liability Management.