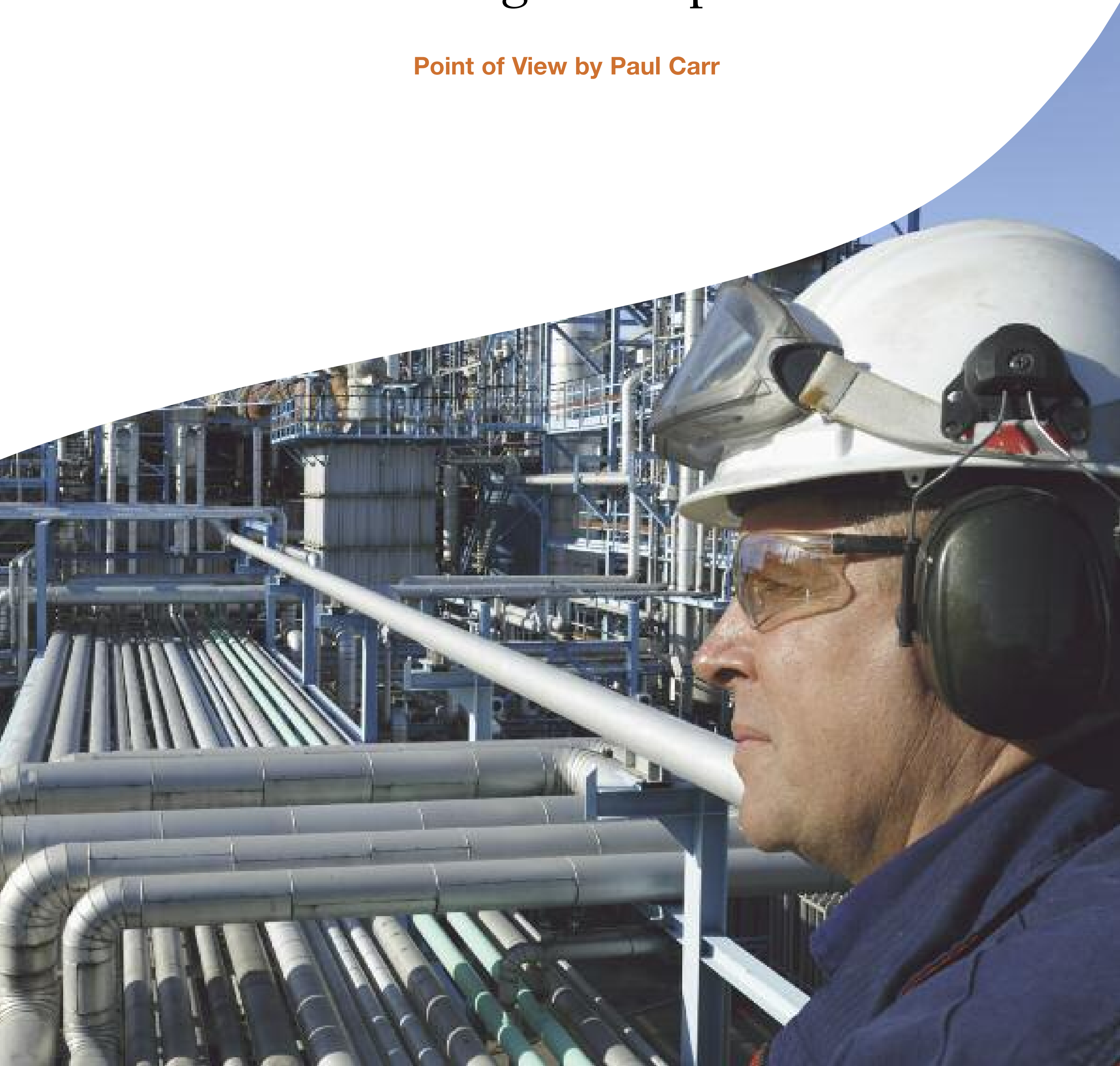
10 security principles for integrated operations

Point of View by Paul Carr



Early estimates from the Norwegian Petroleum Directorate state that 4Q 2008 total production is about 219.5 million Sm3 oil equivalents (o.e.). This is 3.0 million Sm3 o.e. higher than in the same period the year before.[1] Recovering and producing oil and gas has spurred technological innovation and has made the Norwegian Continental Shelf (NCS) an industry-leading region in integrated operations. OLF (Norwegian Oil Industry Association)[2] coined the term 'Integrated Operations' (IO) which means "real-time data onshore from offshore fields and new integrated work processes". OLF has estimated the economic potential of IO to be in the magnitude of €34 billion. Figure 1 illustrates OLF's plan for IO adoption for companies operating on the NCS.

The heart of IO is the continuous flow of secure electronic information between stakeholders; but that isn't always possible for two reasons:

- security incidents are frequent
- security levels vary widely.

This means that as information is pumped through the chain of stakeholders, the risk of security breech is high and the result would be to break the entire supply chain.[3]

The classic Information Systems definition of security focuses on the following security services: Confidentiality, Integrity and Availability[4]. For IO, the security services must include Authentication, Traceability, and Non-Repudiation to cover electronic partnerships. It is important that stakeholders can trust each other to handle all these areas of information security.

This paper lists 10 important security principles to consider when designing or implementing IO related processes or systems to enable companies to exchange information in a trusted and secure environment.

1. Agree baseline security measures between stakeholders

For companies to work together it is critical that all involved parties handle shared information in a secure manner and can trust the availability of services. This means that all parties must acknowledge an agreed level of base security. For further reading, ISO IEC 17799 / 27002 provides excellent examples of base security scenarios. The OLF document: "104 - Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems" demonstrates this concept in IO. The most important part of these documents is the requirement to have a security policy showing the intent and direction for information security, and the requirement to perform risk assessments for the systems used. The OLF Information Security Baseline Requirements (ISBR) tool is available to check compliance against their standard.

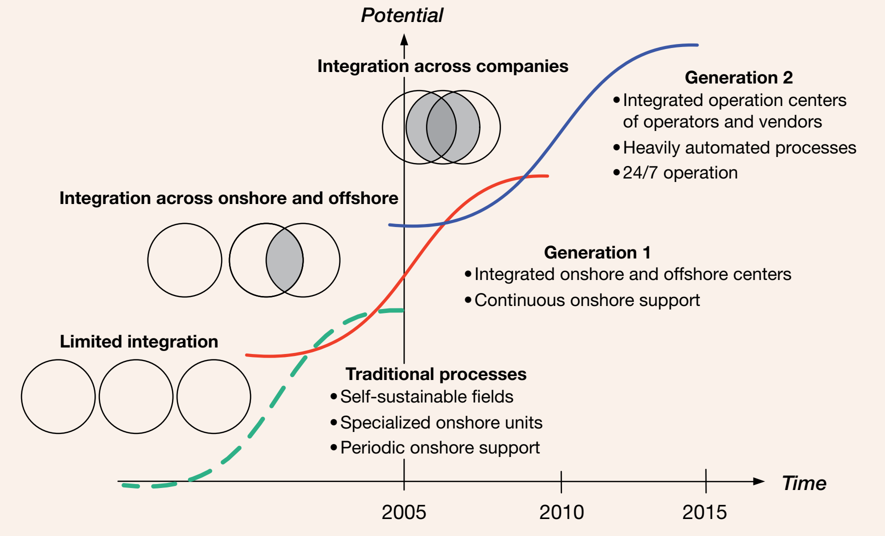
Another alternative is to use the American Petroleum Institute "Security Guidelines for the Petroleum Industry", which is more comprehensive but covers the whole industry.

2. Define clear boundaries of responsibility

In IO, many stakeholders may handle the same data. To be able to agree on how to secure the data, it is necessary to define clear boundaries of responsibility on when and where data is handed over between different parties. This means defining security domains. A security domain is an area where information is handled with the same level of security. Suppose an operator creates a domain called "Operator drilling control domain" where all information is related to drilling operations and owned by the operator. The operator then sets certain levels of security that must be maintained within this domain. For example, one security level could dictate that the availability of services should be 99.8% at all times.

There may be many security domains within one company, depending on requirements. Stakeholders should have their own security domains. Figure 2 shows a security domain consisting of the systems and infrastructure needed for a business function. Typically a company could have a security domain for each business function and one for each

Figure 1: OLF's plan for IO adoption for companies operating on the NCS


Potential
Integration across companies
Generation 2
• Integrated operation centers of operators and vendors
• Heavily automated processes
• 24/7 operation
Integration across onshore and offshore
Generation 1
• Integrated onshore and offshore centers
• Continuous onshore support
Limited integration
Traditional processes
• Self-sustainable fields
• Specialized onshore units
• Periodic onshore support
Time
2005
2010
2015

Source: Oljeindustriens Landsforening (OLF)

[1] http://www.npd.no/English/Aktuelt/Pressemeldinger/2009/2009_1_9_prodtall_nov_08.htm 2009 Press release on estimates for yearly production.
[2] Oljeindustriens Landsforening; http://olf.no
[3] Source: Capgemini's Point of View on Transformation of Process Control Security in the Energy Industry
[4] Ref: ISO 7498-2

geographical area. As a minimum a drilling rig should have its own security domain.

It is particularly important to define the boundaries between security domains. A physical boundary may be easy to define (e.g. at the connection between a router and a cable), but it may also be necessary to define logical boundaries. Physical networks and equipment may be shared, so the boundary when exchanging data may be between logical VPN connections. Note however that it is still important to define who has responsibility for the shared equipment – this still belongs to a physical security domain!

Figure 3 shows an example logical domain where the physical boundaries are not the main issue, but rather the several logical networks are set up as part of one physical network. Typically on a drilling rig with high cost communications to central locations you may share the physical link between several stakeholders who have their own separate logical domains.

Companies often need information that is stored on the intranets of their partners, suppliers or customers. SOIL (Secure Oil Information Link) is a fully managed, members only network hub that enables companies to cost effectively share and exchange information with guaranteed speed, reliability and security, over a North Sea wide network.[5]

The SOIL network Hub is a good example of a security domain with clear boundaries at the firewalls connecting SOIL to the companies using it.

Note that the boundaries of domains need to have some security controls, usually handled by a router or firewall. It should however not be necessary to set up two firewalls next to each other, one for each domain, if you can trust the party responsible for the other domain.

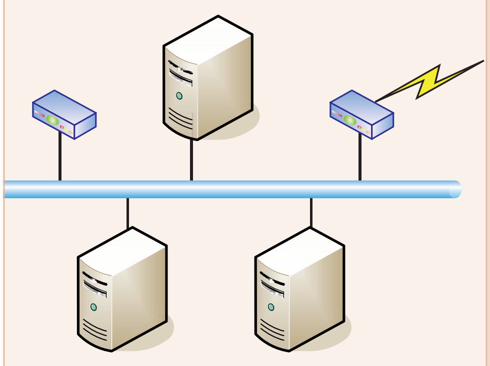
3. Establish contracts

External contracts

Contracts must be established between security domains (internal and external) to define required levels of security within each domain. Chapter 6.2.3 of ISO/IEC 27002 is a comprehensive list of what to include in contracts between two parties:

a) the information security policy;
b) controls to ensure asset protection, including procedures and physical protection;
c/d) training and awareness in methods, procedures, and security;
e) provision for the transfer of personnel
f) responsibilities regarding hardware and software installation and maintenance;
g) a clear reporting structure and agreed reporting formats;
h) a clear and specified process of change management;
i) access control policy;
j) arrangements for reporting, notification, and investigation of information security incidents
k) a description of the product or service to be provided, and a description of the information to be made available along with its security classification;
l) the target level of service and unacceptable levels of service;
m) the definition of verifiable performance criteria, their monitoring and reporting;
n) the right to monitor, and revoke, any activity related to the organization's assets;
o) the right to audit;
p) an escalation process for problem resolution;
q) service continuity requirements;
r) the respective liabilities of the parties to the agreement;
s) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation;
t) intellectual property rights and copyright assignment and protection of any collaborative work;
u) involvement of the third party with subcontractors, and the security controls these subcontractors need to implement;
v) conditions for renegotiation/termination of agreements.

Figure 2: Physical domain consisting of servers, systems, and network segments



Source: Capgemini

Internal contracts

The above list is fairly comprehensive and is a good basis for a contract between two parties. For internal contracts, either between domains or between services inside the domains a less detailed list may be used. The contracts (or level of trust) may simply contain defined levels of Confidentiality, Integrity and Availability, e.g. for each Confidentiality level defining requirements for logical access (passwords, encryption), for Integrity level validation checks, and for Availability levels % uptime per month.

4. Ensure all data has clear ownership

This is a very important base requirement that is often not considered. Without ownership there is nobody to describe the security requirements and the security implementation is purely based on guesswork by the people implementing the solutions. The owner not only defines the security

[5] The SOIL Network was first introduced in Norway in 1998, and quickly became an established communication tool. The network has since expanded to Aberdeen and is now available as a North Sea wide network. Today, the network boasts over 215 companies as registered users, and has expanded to include a wide range of collaboration services. http://www.oilcamp.com/portal/ProductsServices/SOILNetwork/tabid/63/Default.aspx

requirements, but is also responsible for classifying the data according to security policies. This means, at a minimum, to decide the level of confidentiality required for that data.

Every piece of data must have an owner who is responsible for defining what security is required. Usually this can be done at a high level, e.g. ownership could be for all maintenance data, all personnel related data and so on. Sometimes, however, ownership may have to be at a lower level, e.g. different ownership of the various data that is contained in the lifecycle history of some drilling equipment (the equipment owner wants to know what forces it has been influenced by, the operator wants to know the exact coordinates it has been at during drilling).

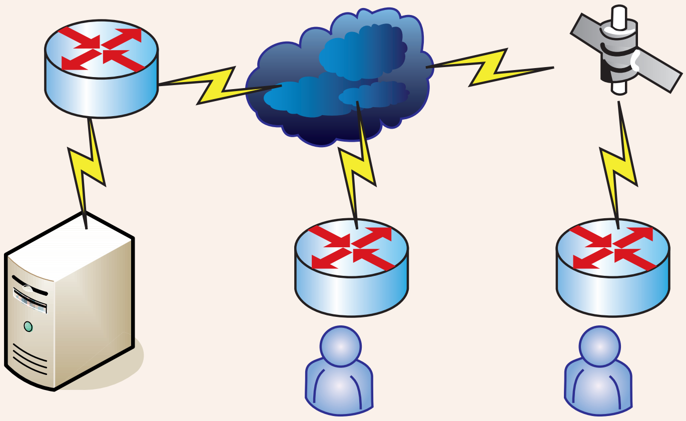
The ownership of data may also change in time, e.g. RFID (radio frequency identification) data may have one owner when being captured as a piece of cargo is scanned during transport, and another owner when handled in a logistics or maintenance system.

The important point, however, is that at all times all data has a clear owner who decides the level of security to be used, where the data is held or whatever security domain it travels through. All parties involved must agree who the owner of the data is at any time.

5. Trust authentication done by source

As people or systems access data or systems across security domains, it is important that one can trust that the person or system is what or who it claims to be. This is particularly important for access into other companies' domains. An example would be an expert at a subcontractor onshore needing direct access to a system offshore. If a contract or trust relationship has been set up between the two companies (or their security domains), then one company should be able to trust the authentication system at the other company: If that company says he is John Smith, then this company will also believe that, and he should not have to authenticate a second time.

Figure 3: Logical domain showing VPN connections for a service/system



Source: Capgemini

This is the basis for federated identity systems, and should be used if possible. The alternative would be re-authenticating whenever passing between security domains, a virtually unmanageable task when frequently crossing domains, which is the case in IO. Federated identity systems are becoming increasingly used exactly for that reason – an example is the more than 80 products that have passed the Liberty[6] alliance testing as federated identity solutions.

Note that even if a user is authenticated at an external source you may still choose to set up separate security mechanisms to limit the access for such users, e.g. use a Demilitarized Zone (DMZ)[7] providing remote access control to specific systems/applications (according to time limitations in approved work permits).

6. Ensure activity logging

During a real-time activity, like drilling or production, it is particularly important to log all activities as they happen, to make it possible to analyze what happened after an incident. This allows learning from mistakes (or learning from what was done well). It may be used to find out what went wrong so it may be corrected, or it may be to detect security incidents. Also, it may be impossible to react fast enough to handle the event in real-time, but using the log of what happened allows proper correction before further damage is done. The log itself should contain information about what happened, who (or which system) was responsible, when it happened, and what system it affected. The level of detail for the logging may be set according to what is practical and useful. The logging is normally best performed by the applications themselves – this needs to be specified as part of the requirement for a new application.

Analysis of the log can be partly automated if required, even with automatic action to correct the problem (e.g. using Intrusion Prevention Systems). It is, however, important to decide when and how logs should be analyzed, and implement that decision. The decision on what to analyze should be based on a risk assessment. Logs that are not used are purely a resource drain.

[6] See: http://www.projectliberty.org/ - this is an organization that has established standards to ensure that federated identity solutions can work together.
[7] DMZ = Demilitarized Zone, meaning a separate domain that can be accessed from outside and is protected separately.

You also may need to share log information to integrate monitoring across the borders of the organization – proper analysis may not be possible without access to all data. Note, however, the need to safeguard the logs for forensic and incident investigations.

There is no such thing as 100% security, so logging what happens is an additional safeguard to handle events that shouldn't have happened in the first place.

7. Establish multilayer protection

Due to the fact that it is impossible to achieve 100% protection, it is wise to protect at multiple layers. Ideally any item should only need to be protected at source – e.g. a database or data store should maintain its own protection (in practice this would normally mean encrypting the data). Knowing that this is never enough, one should also protect the system accessing the database, the computer running that system, the security domain that contains that system, the borders of the company network, and the borders of the industry network (e.g. the SOIL network).

These layers of security will make it more difficult for hackers (crackers) or viruses (or any malware) to cause harm, without making it unnecessarily difficult to perform normal operations.

8. Be open

Security by obscurity does not work. This has been shown in practice many times – the safest systems are often those written as open source, where anybody can inspect the code and point out or correct security flaws.

More importantly – use open standards and open security mechanisms, e.g. PKI based encryption where the basic algorithm is well known but still unbroken, the TSL communication protocol, an IETF standard, or the lower level IPsec communications standard.

Also: there are many security tools that rely on contributions provided in the open community – these are often tools that lead the way in the realm of IT security and can be used to ensure the security of your systems.

The Jericho forum describes how to implement the deperimeterization concept and gives some ideas how it can be done in a standard and open way[8]. They have also defined "Commandments" similar to the 10 security principles in this paper but to be used in general situations of deperimeterization.

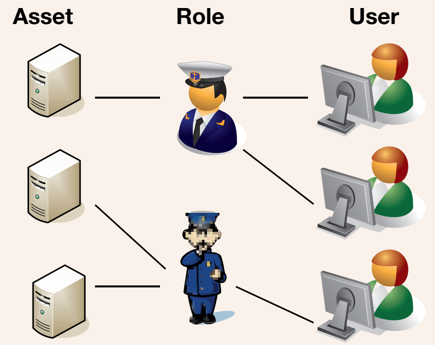
9. Use role- and asset-based access

Historically access control has been straight forward by setting up user X to allow access to asset Y. When you have many users and many assets, and the users keep changing their roles (e.g. often offshore users may have many roles) this gets very difficult to maintain, and even more difficult to check if it is correct.

The current best practice for access control in the oil industry is role and asset based access control. This means that for each overall asset (an overall asset being for instance an oil field or platform), several roles are defined. The access required to perform the functions for that role is then defined, e.g. a driller needs access to drilling systems, and a maintenance engineer needs access to maintenance systems.

A new user (or system) is then given access to the systems or assets that is required for the role(s) performed, and as roles are changed or added, the access is changed accordingly – you only need to know what roles are performed – not the details of access required, these have already been defined as part of the role definition. Figure 4 shows how users, roles and assets may be linked together.

Figure 4: Role and asset based access



Source: Capgemini

Ideally this access system could be extended to context based access where the situation the user is in is considered, e.g. if the user is accessing systems from a laptop during travel (rather than in the secure work environment) he should not get the same access.

10. Show social responsibility

As in any situation where you interact with other parties, it is important to follow some simple rules for the interaction to work well:

- Don't be the one infecting the other parties with virus or spam. Ensuring base security as explained earlier will help, but also make sure that firewalls and routers are set up to stop unwanted traffic both ways – not just inbound traffic.
- Do not spam or overload the other parties with unnecessary traffic. Send the data that is necessary for the work in hand, and only that. It is easier and more efficient to remove unneeded data at the source than later.
- Ensure that when an incident occurs you can work together across organizational boundaries to solve the issue.

A security policy should be produced and used as a basis to raise awareness of information security and of the risk associated with information exchange.

[8] See http://www.opengroup.org/jericho/ for details

As Thore Langeland, Manager Integrated Operations at OLF says:

"Information Security is very much about attitude and behavior in the daily work. So the last security principle in this document - show social responsibility - is one of the more important principles. For this reason OLF has made some mnemonics for the individual in a brochure available on OLF's web site[9]."

Conclusion

The 10 principles in this paper are all about defining domains of security and protecting those domains and the information within. These are important principles that are necessary to protect the information, and following these principles will help ensuring appropriate protection.

The 10 principles are repeated here:

1. **Agree baseline security measures between stakeholders**
2. **Define clear boundaries of responsibility**
3. **Establish contracts**
4. **Ensure all data has clear ownership**
5. **Trust authentication done by source**
6. **Ensure activity logging**
7. **Establish multilayer protection**
8. **Be open**
9. **Use role- and asset-based access**
10. **Show social responsibility.**

Today in the Oil and Gas Industry there are some companies that have made a lot of progress in addressing these principles internally. However many companies are lacking in most areas. Once several stakeholders are included the total solution will normally have very weak security that it which will take a long time and a lot of effort to correct unless it is considered up-front. This weak security may even be a showstopper for an important collaboration process between stakeholders and therefore prevent major savings being made (ref the €34 billion savings estimated on the Norwegian Continental Shelf as mentioned at the beginning of this paper).

Note that IO is about integration of a supply chain across several domains, possibly across several stakeholders. It is also important to manage the big picture, and ensure that the whole information flow functions according to the intended purpose. This big picture covers the integration part of IO, and is not covered here – it is all about proper architecture, and managing the orchestration of information as it flows between systems and people.

[9] http://www.olf.no/getfile.php/zKonvertert/www.olf.no/Rapporter/Dokumenter/071030%20Informasjonssikkerhet%2C%20brosjyre.pdf

References

- **ISO IEC 17799 / 27002:** http://www.iso.org/iso/catalogue_detail?csnumber=50297

- **104 - Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems** - http://www.olf.no/101-120/104-information-security-baseline-requirements-for-process-control-safety-and-support-ict-systems-article876-1364.html

- **OLF IO architecture:** not published yet, but available on request

- **Capgemini security services:** http://www.capgemini.com/services/technology-services/security/

- **Federated identity:** http://en.wikipedia.org/wiki/Federated_identity

- **SOIL network:** http://www.rignet.com/Solutions/SOIL/The_Network/

- **RFID OLF:** not yet published in April 2009. See http://olf.no/

- Capgemini's Point of View on **Transformation of Process Control Security in the Energy Industry:** http://www.capgemini.com/resources/thought_leadership/transformation_of_process_control_security_in_the_energy_industry/

- **Jericho forum:** http://www.opengroup.org/jericho/

- **API - The American Petroleum Institute:** http://www.api.org/policy/otherissues/

www.capgemini.com/energy

About Capgemini and the Collaborative Business Experience™

Capgemini, one of the world's foremost providers of consulting, technology and outsourcing services, enables its clients to transform and perform through technologies.

Capgemini provides its clients with insights and capabilities that boost their freedom to achieve superior results through a unique way of working, the Collaborative Business Experience™. The Group relies on its global delivery model called Rightshore®, which aims to get the right balance of the best talent from multiple locations, working as one team to create and deliver the optimum solution for clients. Present in more than 30 countries, Capgemini reported 2008 global revenues of EUR 8.7 billion and employs over 90,000 people worldwide.

With 1.2 billion euros revenue in 2008 and 12,000+ dedicated consultants engaged in Energy, Utilities and Chemicals projects across Europe, North America and Asia Pacific, Capgemini's Energy, Utilities & Chemicals Global Sector serves the business consulting and information technology needs of many of the world's largest players of this industry.

More information about our services, offices and research is available at **www.capgemini.com/energy**

EPiCentre
Exploration and Production Industry Competence - Centre of Excellence

SSC-ST 2009 May

For more information, please contact:

Paul Carr
paul.carr@capgemini.com

Head of Epicentre Capgemini Norge
Jens Middborg
jens.middborg@capgemini.com

Global Oil & Gas Centre of Excellence
Ian Moore
ian.moore@capgemini.com