The Petroleum Safety Authority Norway

Protection of data at rest and in transit

Authors:
Andreas Grefsrud, Kenneth Titlestad, Øystein Aspøy, Kristin Weiseth, Kari Anette Sand

Contents

1 Summary

This report summarises knowledge and experience from the petroleum sector relating to the protection of data and information. Various key perspectives that are of relevance to this are also discussed. The starting point is that data must be protected while at rest and in transit and that developments in digital technology, both within and outside of the sector, create greater complexity, new vulnerabilities and changes to the threat landscape. Data and information security are becoming more important, and the result of this is that the sector is being challenged on its knowledge development and processes for management, control and risk management. The type of technological development referred to as Industry 4.0, which involves OT being closely integrated with IT and cloud services, provides opportunities for better control of a complex picture of deliveries, systems and data flows between suppliers and operating companies, however also entails greater complexity, longer value chains and more uncertain factors in relation to information security, IT security and general safety work. The discussion in this report looks at the related human, technological and organisational vulnerabilities which the petroleum sector is facing and what key processes may need to be strengthened in order to achieve good information security and IT security work.

2 Introduction

2.1 Background to the project

The purpose of the assignment was to be able to provide an answer to the question of the extent to which data and information are protected, both while at rest and in transit.

The greatest amount of knowledge about technological solutions for storing and transferring information is often possessed by one or more providers. This creates dependencies between providers at several stages. Cloud, data lake, SaaS and more recent mechanisms for data transport, both wired and wireless, present opportunities for more provider-driven deliveries and operating contracts in the digital value chain. This interconnection between multiple systems and solutions involving multiple actors contributes to even more complex supply chains. The degree of complexity and dependencies in these types of supply chains make it more difficult to obtain a good overview and knowledge of information assets and owners, vulnerabilities, threats, the probability of incidents and attacks, as well as potential consequences. Such dependencies may result in chain reactions occurring that have consequences for the entire value chain.

In order to provide an answer to how data and information are protected, this assignment has focussed in particular on the interaction between the operators and other actors in the petroleum sector. This assignment considers whether risk ownership is adequately safeguarded, whether management and control are with the operators, or whether these tasks are left to providers and how this impacts risk and opportunities for control.

2.2 Terms, definitions and abbreviations

2.2.1 Terms

Term	Definition / Description
A-Standard Action Pattern	Equinor's action pattern, which describes how to plan, execute and evaluate a specific job or activity at its best, in order for it to be executed correctly the first time. [1]
Data diode	A network communication device which uses optics and/or electronics to transport data in only one direction.
Digital twin	A digital representation of physical objects, systems and processes.
DIKW	Data – Information – Knowledge - Wisdom is a model which depicts the manner in which we

	move from data to information, knowledge and wisdom through decisions and actions.
Edge	Term for calculating and data processing in close proximity to the data sources. This is most often a server or computer offshore.
Extractor	Solution which has the function of retrieving data from one or more systems and transporting this to another system.
GDPR	The General Data Protection Regulation (GDPR) is a regulation for the protection of data and privacy when processing personal data in the European Union (EU).
Integrity	Reliability and accuracy of data/information.
Internal control	Comprehensive business process rooted in management, which contributes to targeted and efficient operations, reliable reporting and compliance with regulations.
Confidentiality	Level of sensitivity of data/information which entails that it must not be disclosed or made available to unauthorised parties.
Model Based System Engineering	A model for formalised use of modelling to support the stipulation of requirements, design, analysis, verification and validation.
Privacy	Privacy concerns the right to a private life and the right to control the use of one's own personal data.
Risk owner	Role that has been delegated responsibility for performance. The role is responsible for both good and poor results within the area of responsibility, and therefore owns the risk within this area.
Syslog	A standard for message logging within data processing.
Availability	A measure of whether data/information is available to those who require it.
Enterprise	Common term for a public administrative body or private company with or without a board of directors.

Business management	The management of the enterprise, either the CEO/managing director alone, or the senior management team.

2.2.2 Abbreviations

Abbreviation	Description
AMQP	Advanced Message Queuing Protocol
INL CCE	Idaho National Lab's Model for Consequence-Driven Cyberinformed Engineering
CIA	Confidentiality, Integrity, Availability
COBIT	Control Objectives for Information and related Technologies
DDoS	Distributed Denial of Service
EPC	Engineering, Procurement and Construction
FTP	File Transfer Protocol
HAZOP	Hazard and Operability
HMI	Human Machine Interface
HSE	Health, Safety and the Environment
ICS	Industrial Control Systems
IMS	Information Management System
IoT	Internet of Things
ISMS	Information Security Management System
IT	Information Technology
LOPA	Levels of Protection Analysis
MQTT	Message Queuing Telemetry Transport
NOA	Namur Open Architecture
OPC UA	OPC Unified Architecture
OSINT	Open Source Intelligence
OT	Operational Technology
PHA	Process Hazards Analysis
PIMS	Production Information Management System
PLC	Programmable Logic Controller
SaaS	Software as a Service
SFTP	SSH File Transfer Protocol
SIS	Safety Instrumented system
SSH	Secure Socket Shell

2.3 Methodology and implementation

The project applied qualitative methodology when carrying out this work. In-depth interviews were conducted with key suppliers and companies in the petroleum sector. There was also a literature review, and the information that was collected has been systematised and analysed. The in-depth interviews and literature review ensured that important information could be collected from various sources, while also providing the basis for analysis, discussions in the report and recommendations. Sopra Steria used its own interdisciplinary team consisting of specialists in OT/IT, information security and risk management during all phases of the project to ensure professional quality in the collection and processing of information.

2.3.1 In-depth interviews

In-depth interviews were conducted with important companies and personnel in the petroleum sector that have relevant knowledge about the current initiatives, status, challenges and opportunities. The interviews were carried out as semi-structured interviews for which a set of questions and an interview guide were prepared in advance. All of the respondents received the same questionnaire and most of the questions had already been responded to in writing prior to the interviews. The written responses provided by the respondents were then verbally reviewed together with them, a process which provided scope for further dialogue regarding the original questions. The starting point for the interviews was the interview guide, as well as questions not included in the guide that were formulated and adapted to each respondent depending on the responses given to the questions and where the actor was located on the value chain.

A well-considered selection of companies was made to ensure that there was a representative and broad sample of the petroleum sector and the value chain. Interviews were therefore conducted with various operating companies and suppliers. Several companies collectively covered the roles of:

- Operating company
- Contractor company (EPC)
- Supplier of industrial control systems and safety instrumented systems
- Supplier of solutions for industrial digitalisation (Industry 4.0)

2.3.2 Literature review

The literature review included a review of relevant and updated information from guidelines and previous knowledge reports. This includes relevant reports in recent years from the International Research Institute of Stavanger (IRIS), Sintef, DNV and the Norwegian Directorate for Civil Protection (DSB), as well as more recent editions of international standards, including IEC 62443, ISO 27001, ISO 27002, ISO 27005 and ISO 31000.

2.3.3 Analysis

Information from in-depth interviews, the literature review and the experiences of specialists in the project was collated for analysis. This forms the basis for the discussion in the report and the recommendations that are given.

3 History and background

The technological developments that have taken place in recent years, specifically developments in industrial digitalisation and Industry 4.0, have enabled the petroleum sector to see increased opportunities to apply digital technology across OT and IT, across operators/suppliers and through larger parts of the operating life of facilities and equipment. New systems are being developed and brought online to improve the ability to design, construct, monitor and maintain facilities and equipment from decentralised locations at one or more suppliers in a digital value chain. Drawings, models, configuration and time series data are combined, contextualized and enriched into new information. This is information that is sought to be made available in a growing digital value chain that extends from sensors, via industrial control systems and Edge and/or office systems, to cloud-based data platforms with operators and suppliers. By enriching data from multiple sources, models and decisions can be given stronger basic data and be better suited for direct or indirect monitoring and management.

However, during this technological journey it is unclear as to what extent the actors along the digital value chains are aware of inherent risks and whether they ensure that data and information are adequately protected, both during transfer (transit) and when being stored (at rest). It is also unclear as to whether the various actors are aware of their role in the value chain, and whether the responsible operating company adequately follows up and safeguards both its own and suppliers' control and risk management of data and information.

The petroleum sector has historically used industrial control and safety systems that are separate from other IT systems. The risk picture for these systems has largely been manageable. However, the emergence of cloud, IoT/IIoT and other technological advances has created opportunities for better efficiency and optimisation within engineering, monitoring, control and maintenance. The stage has thus been set for a development in which previously isolated systems (Purdue levels 1 to 3 in Figure 1) are now linked together and enriched with functions in cloud services from one or more providers. This contributes to creating a more complex and convoluted picture of ownership of services and information. It is a challenge to assess what risks this may introduce and what control and safety mechanisms may contribute to reducing these types of risks.

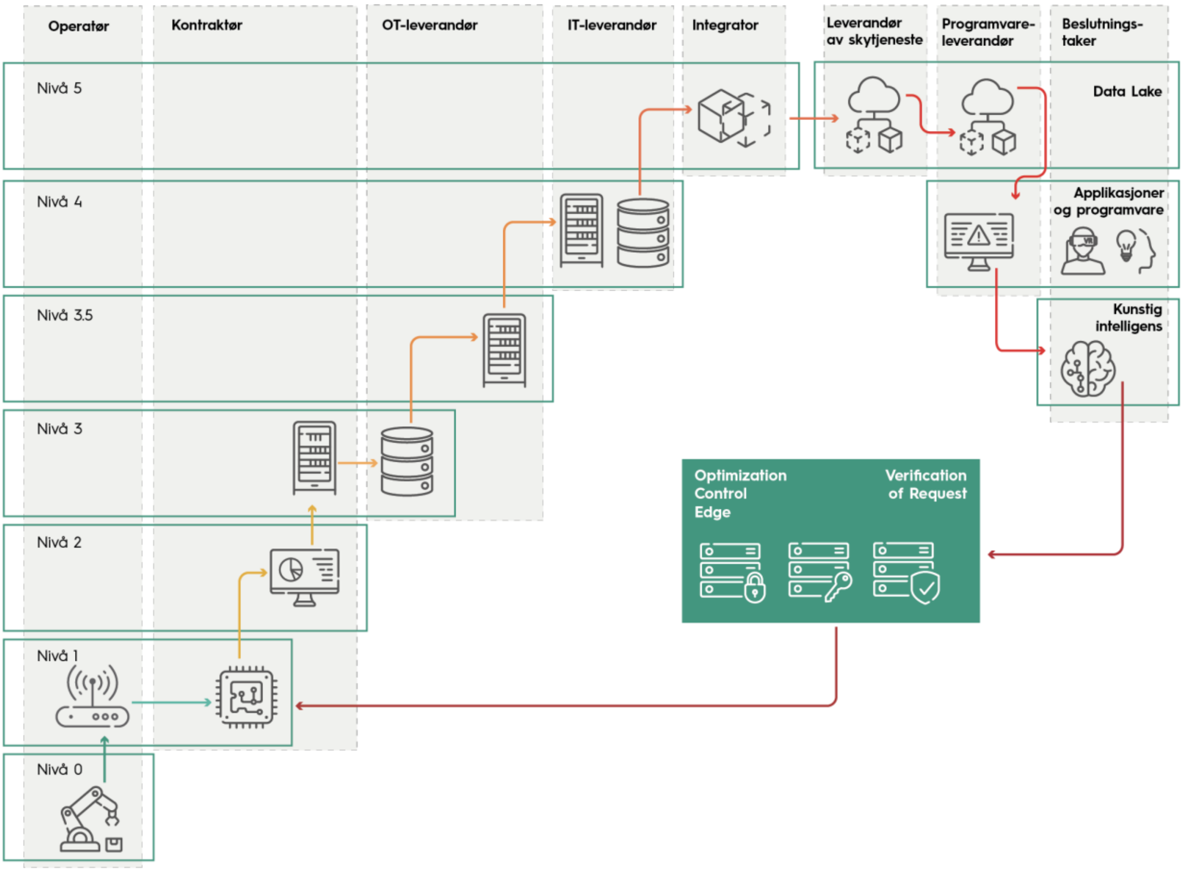

Figure 1: Sensor data is sent out of the control system and to the cloud for advanced data processing. The supplier landscape becomes more complex, the complexity increases and data quality becomes more uncertain. The general risk associated with information security may increase in line with the complexity.

4 Information regarding facilities and systems

Large quantities of data are used and are necessary for operating and maintaining oil and gas installations. As shown in Figure 2, by viewing data correctly and in the right context, it will be possible to provide information - which in turn forms the basis for knowledge, decision-making and action.

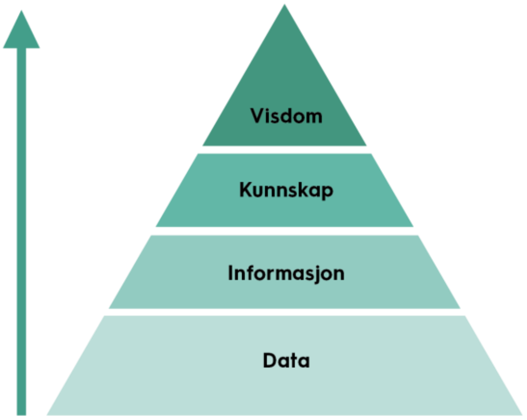

Figure 2: The DIKW model shows how we enrich the data through more information about the data, knowledge and wisdom. This makes it easier to make better, informed and data-based decisions.

Both people and ICT systems use data and the information that can be derived from data as a basis for making decisions and making the correct or optimal decisions.

It is thus a prerequisite that the data is correct, complete, up-to-date, read at the right time and understood correctly. The same applies to metadata - data which describes data - to provide necessary, adequate and proper context. Errors or lack of context for data can result in inadequate or completely incorrect information, which in turn can lead to incorrect decisions and actions.

In interviews and conversations, similar meanings were generally assigned to the terms “data” and “information”. With the emergence of models, for example, those used in Model Based System Engineering, and aggregation/contextualization of data, we also see that it has become more difficult to clearly differentiate between what is data and what is information derived from data.

With the prerequisites that apply to information and decision-making, there is a possibility that data or metadata may be deficient, incorrect, falsified or not available when required. For data that may reveal sensitive information, there is also a risk that this data may become accessible to undesirable parties. Security objectives for data and information are therefore often categorized into Confidentiality, Integrity, Accessibility, and abbreviated to C-I-A. These terms are also normally used in the petroleum sector.

For typical IT systems, there are some instances in which confidentiality and integrity take precedence over availability, see Figure 3. This often comes as a result of IT systems storing and processing personal data or other information that requires protection of confidentiality. Therefore, data protection is also vitally important in security work related to IT systems.

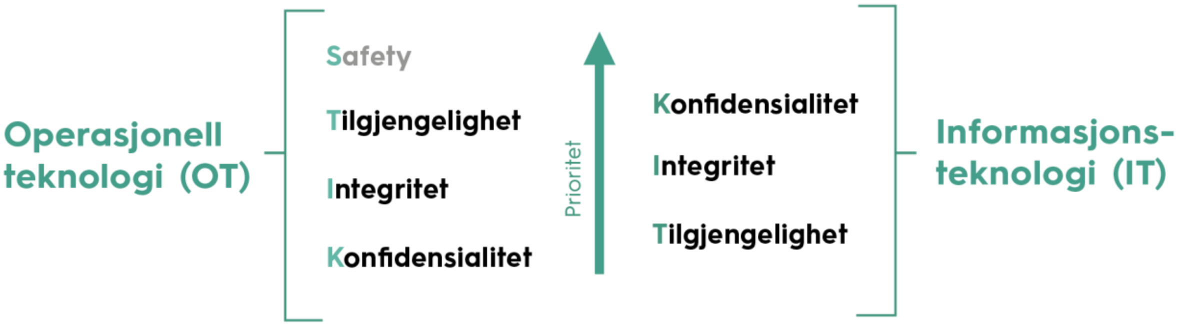

Figure 3: General priorities for the security objectives when concerning typical OT systems vs. IT systems.

However, with the emergence of the internet, and the increasing dependence being assigned to digital services and digital value chains, we are seeing increasing demand for availability for IT systems [2].

For Operational Technology (OT), the processing of personal data is not of key importance. The primary function of OT systems is to monitor, control and manage physical processes. In the OT domain, process values, configuration data, logic, drawings of machines and systems are the focus and are therefore handled with care. This data is used to ensure the safe, stable and efficient operation of facilities and industrial processes. Therefore, because of this objective, availability and integrity are much more important than confidentiality in OT. In some instances, safety is also highlighted as a security objective to illustrate that this is an overarching objective in instances of conflict.

When data is transferred out of the industrial control systems, and the purpose of the transfer is to be able to carry out analyses, reporting and optimisation, the change in purpose entails that the requirements for availability are often reduced. At the same time, the number of transport stages and transactions increases, which is a factor that contributes to greater exposure of data and information. This means that ensuring confidentiality and integrity is becoming increasingly more important. In this sense, data must be protected with regard to C-I-T, both while at rest and in transit, and that the weighting of the security objectives may differ depending on the objectives in the domain in which they will be used. Assessments of risk must therefore be made based on the relevant objective and domains. Perspectives on risk assessment are further discussed in Chapter 8 – "Risk and risk management".

4.1 Different types of data and information

Within the petroleum sector, there are a number of different types of data that are stored and transferred. In this report and in interviews we have chosen to group data into static and dynamic data. This is not intended to be a precise distinction, but is used as a term for referring to two partly different groups of data, information and systems.

Static data and information: Data that is primarily at rest, i.e. stored. This often involves larger quantities of data, which are stored and transferred in bulk, contain a great deal of information and often have some contextual information. Examples of this include technical drawings/forms, configuration files, program files, security updates, and logic and project files.

Dynamic data and information: Data that is primarily in motion, i.e. during transfer. These are often small fragments, values or messages and are often part of a stream of data such as time series, however can also be commands, messages, signals or API calls. Dynamic data often contains little or no contextual information. Examples of such data may include meter readings from transmitters, signals to or from PLCs, communication over Modbus TCP, OPC DA, or through message-queue-based protocols such as AMQP or MQTT.

When communicating over OPC UA, stricter requirements are set for communicating context/metadata in parallel with signals/messages. Data and information in this communication protocol are therefore considered to be a combination of static and dynamic information.

4.2 Systems and sharing of information

The petroleum sector uses a number of different systems for both static and dynamic information, including for internal use in the company and for sharing data and information between companies. For static data and information, which are primarily at rest, internal file sharing areas, document management systems, engineering tools, generic databases and dedicated database-based solutions for requirements, design/engineering, work processes, etc. are used.

The respondents reported that it is preferable to use dedicated document management systems for sharing static information. Several different systems are used for being able to share information across companies in a controlled manner. Access control is therefore primarily managed by the information owner or premise provider, most often the operating company. Examples of these types of solutions that are presently being used in the sector are ProArc, ProcoSys, Documentum, D2, STID, Meridian, Intergraph, PIMS, Aveva Suite and SharePoint (On-Premises). The solutions have varying degrees of functionality for access control, information classification and sharing.

The interviews paint a complex picture of systems, as well as challenges with inadequate functionality. This picture is further confirmed by the fact that most of the respondents also reported that other systems and channels are used for sharing, such as email and FTP/SFTP. The developments in Office 365 in recent years have also resulted in more storage and sharing of information through Sharepoint Online, Teams and OneDrive. The COVID-19 pandemic and use of home office have further reinforced this. Respondents also reported that rigid or cumbersome access controls mean that users sometimes use Dropbox, Google Drive and the like, and often on private accounts. The sector does not appear to have sufficient oversight or control over other sharing channels that are used beyond document management systems.

One challenge reported was that information classification and access control do not automatically accompany information objects if they are copied to another system or to another channel. When access-controlled, sensitive information in a document management system is copied out and shared via Teams or OneDrive, the original information classification and access control become fragmented. A solution to this challenge may be to protect the information from being copied out, for example through restrictions on access and by using the functionality for Digital Rights Management/Information Protection. With this type of solution, for example, Microsoft/Azure Information Protection, there are options for encrypting information objects to enable these to still be copied and shared by them only being able to be decrypted and read if one has the correct access and decryption keys. However, this requires that the systems that are used for sharing support the relevant mechanisms for encryption and decryption. We see that extensive work is required to convince a wide range of companies to agree on what mechanisms should be used for encryption/decryption, as well as implementing and adopting these. Microsoft's solutions in Azure and Office 365 (Azure/Microsoft Information Protection) appear to be most prevalent in the petroleum sector across the value chain. This is similar to what we also experience from other sectors.

A security mechanism used by several companies is to leave information in the source system and grant the relevant users access through remote access. Examples of this are portal solutions such as Citrix, both for IT and for OT. Users sign in to a portal and from there proceed to specific systems in order to access information. Access to more comprehensive line-of-business systems, IMS, and HMI/operator stations will most often be granted in this manner. Due to greater interest in transferring sensor data out of facilities and to the cloud, both the interviews and various projects have revealed an inclination towards increased use of remote access. This is to implement various solutions for data transport, as well as to conduct quality controls or further investigations where data in the cloud appears to be deficient, incorrect or incomprehensible. In the longer term, provided that the sector is able to strengthen the data quality and information in cloud solutions and digital twins, there may be opportunities for reduced use of remote access.

In most cases, the remote access solutions in the sector are highly exposed on the internet. Since they also have a function in securing information/systems worthy of protection, these solutions therefore also pose a significant risk factor for information security, IT security and potential major accidents. At a minimum, these types of solutions must be resistant to threat actors with moderate capacity. If there are not adequate quality controls and maintenance of other key security mechanisms and barriers, for example, the segregation between IT/OT and process control/safety instrumented systems, it is our view that the remote access solutions must also be resistant to determined threat actors that possess significant capacity. By securely transferring the necessary data and information out of the facilities, and enabling the use of secure cloud solutions and digital twins, it may also be possible to achieve benefits for safety and security.

By their very nature, dynamic information and data, such as time series and signals, are largely in motion ("transit"). Data is to a large extent exchanged between endpoints and systems, albeit currently to a lesser extent across companies. Based on interviews, we can see that it is still the case that this exchange primarily takes place within given layers or specific channels in accordance with a traditional Purdue Model, for example, internally in a supplier-specific control system or from and to a limited and controlled number of systems/endpoints. Examples of systems with this type of data exchange are within industrial control systems, onshore control rooms, safety instrumented systems, IMS, Osisoft PI, and between one or more such systems. There is also data exchange at PLC level between operating companies, for example for control and management of electrical power, and for processing facilities that are dependent on one another across facilities and operating companies.

Due to the initiatives taking place in Industry 4.0, there is an increase in ongoing efforts to extract data flows out of the facilities. It is preferable to do this in the form of the OPC UA, AMQP or MQTT protocols, however other mechanisms are also used, such as file copying over FTP/SFTP, database replication, syslog or through other more proprietary mechanisms. Data transport takes place through dedicated data gateways and extractors. Data diodes are used to a very limited extent, however, several actors reported that they are considering adopting the use of these. A number of actors also expressed interest in Namur Open Architecture (NOA), including NOA Diode. Data is transported to industrial data lakes in the cloud, such as Omnia, Cognite Data Fusion, Kognifai, Veracity, etc. There are also investments being made in and pilot projects for obtaining data for various SaaS solutions, and being able to establish digital twins and Asset Administration Shells.

The respondents appear to be aware of certain risk factors associated with the focus on Industry 4.0, for example, how important and difficult it is to ensure data integrity and data quality. Certain respondents also expressed some concern about how data transport channels are constructed and implemented, and that allowing data transport out of secure zones increases the risk that threat actors could exploit known or unknown vulnerabilities to hack their way in. However, with incidents such as SolarWinds/Sunburst, Triton and the Ekans virus fresh in our minds, it is our opinion that the latter-mentioned topic does not receive enough attention in the petroleum sector. There are sometimes discussions in the sector about security mechanisms for OPC UA, vulnerable protocols, data diodes and NOA Diode, however little attention is still devoted to these matters when compared with the focus on information models, interoperability and digital twins. Extensive security assessments should be carried out for data gateways and for how OPC UA, AMQP and MQTT will be protected. When concerning solutions for NOA Diode, there also needs to be a review of the security design, prerequisites, build quality and weaknesses.

Some respondents reported that it is a very complex task while making this technological journey to obtain a good overview and knowledge of information assets and owners, vulnerabilities, threats, probability of incidents/attacks and potential consequences.

5 Industry 4.0

Industry 4.0 is used as a term to describe the Fourth Industrial Revolution that will involve the use of advanced technology, digitalisation and interoperability to fully automate and robotize production and industry across value and supply chains.

The petroleum sector has a long tradition of automating and controlling processes and operations using automation and technology. There is also a good history of moving data onshore for analysis within the areas of drilling, exploration and production of oil and gas. The next evolution may be autonomous systems that communicate and make decisions beyond the functionality that individual PLCs currently possess. This will be an approach to management without control rooms and operators, and which is based on data analysis and autonomous management.

To achieve this, decision-making systems require a richer stream of data than what has hereto been the case – often without compression or processing of data, and with more metadata, information on data quality and other information from multiple sources. These types of data streams are often sent to one or more cloud services for analysis, and/or to office-level systems where there are also simulation programmes and other programmes that do not necessarily run in an isolated system as was previously the case.

The petroleum sector has incorporated the Purdue Model (see the simplified version in Figure 4) as an approach for ensuring the integrity of industrial control systems. The model is primarily designed to be able to describe various functions in the industrial system, and it was not intended to serve as a model for security. It has nevertheless proven to be highly applicable for security purposes for OT. It is used as a guide to physical architecture design and is frequently referred to as a blueprint for how critical infrastructure can be protected.

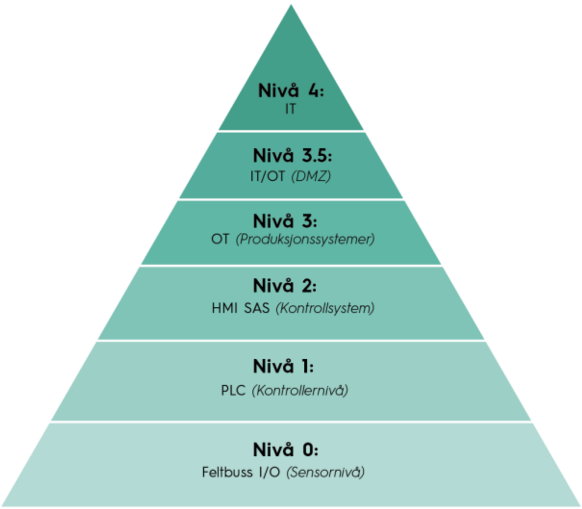

Figure 4: Simplified version of the Purdue Model.

5.1 Observations and discussion

Industry 4.0 is now challenging the use of the Purdue Model as a blueprint for security for OT systems. Level 2 is going to be more dispersed, which is something we are already seeing, for example, in drilling and well maintenance, where equipment is now placed on the installations for monitoring, logging and enriching the information directly from wells and equipment in wells. In some instances, this is also connected directly to the control system for the wells, which in turn are often connected directly to the platforms' main control systems.

We see examples of "Edge equipment" being installed on industrial equipment to log data and which often communicates with a service outside the industrial environment to enrich data and provide users with a better analysis of the data in real time. We also see the fragmentation of the Purdue zones within the larger control systems, despite most of the examples currently sending a richer stream of data from level 2 to the cloud and thereafter being presented in an application or service that the operators in control rooms use for analysis/support, or as a guide in the operation of the industrial processes.

For solutions constructed in accordance with the Purdue Model, it is important that there is a movement in the future towards "Zero Trust" in order to protect data streams while also controlling what devices, people and systems are able to do - in the form of controls of identities/accesses, rights to execute code, rights to operations in HMI, etc. There is presently not much of a system in terms of restrictions on what can be done as long as one has network contact with controllers and industrial systems. When data streams to the cloud are not adequately secured, this increases the possibility that unauthorized parties, for example hackers, may be able to operate and reprogramme both process control and safety instrumented systems from remote locations, with the potential to cause damage and harm to machines, facilities, people and the environment. Through reconnaissance and a step-by-step approach from a determined threat actor, the potential for harm can be catastrophic, and with the current prevalence of programmable digital technology, there is no certainty that there are sufficiently unprogrammable or independent barriers to prevent or limit such an accident.

Everything is going to be in a continuous state of change in the future, and with the current change management in heavy industry, there is a gap between what has been installed and is in operation and what has been documented. It should be considered as to whether to employ the use of more modern, dedicated tools – which are being used in software development – for change and version management to avoid ending up with outdated and incorrect documentation.

Furthermore, functions should be implemented at endpoints that limit the assets that can be changed and what one generally should be granted access to. Attempts should also be made to move away from privileged access, with rights that exceed what is necessary. It is fully possible to protect accesses, both for read-only access and write access. But how does one ensure trust between sender and recipient?

Moving into the future, there will probably be fewer static systems that are only configured and put into operation. An example of this is equipment that is currently isolated with a local controller/PLC. This is equipment that has not previously been connected online or has not had security updates. In the future this type of equipment will be connected to the internet and communicate with solutions at other locations for optimization. To ensure the integrity and availability of modern industrial systems it will be of crucial importance that there are wellfunctioning mechanisms for access control, authentication and other technical security mechanisms. In order to determine an adequate level for these mechanisms and ensure that they remain at this level at all times, it is essential to ensure that processes and compliance are rooted in a good understanding of risk and dealt with through good risk management. These are the topics for the next chapters of the report.

6 Information security

It is clear that the vast majority of companies in the sector rely on information and data to be able to execute their operations. Information takes both oral and written form and is it is stored and transported via analog and digital systems and solutions.

Information and data that are part of and influence all processes, activities and decisions should be protected in a manner that contributes to the companies achieving the results that the owners and society expect. This includes the expectation that accidents will not occur, or that society will suffer other negative externalities as a consequence of the sector's operations.

Data and information therefore have a direct impact on the companies' results and regulatory compliance. In other words, the more important the information, the greater the consequences can be in both the short and long term if it is incorrect, cannot be accessed or gets into the hands of unauthorised parties. As shown in Chapter 4, information security is about ensuring the:

- integrity,
- availability and
- confidentiality of the information.

Which of these three dimensions is most important must be balanced according to the needs of the company and society.

There are primarily two factors that influence information security: threats and vulnerabilities, see Figure 5. The appropriate measures to implement in order to reduce the level of vulnerability and thereby prevent a threat actor from achieving its objective, correlate with the value of the information or data in terms of potential benefits and/or harm, both for information owners, and for the threat actors.

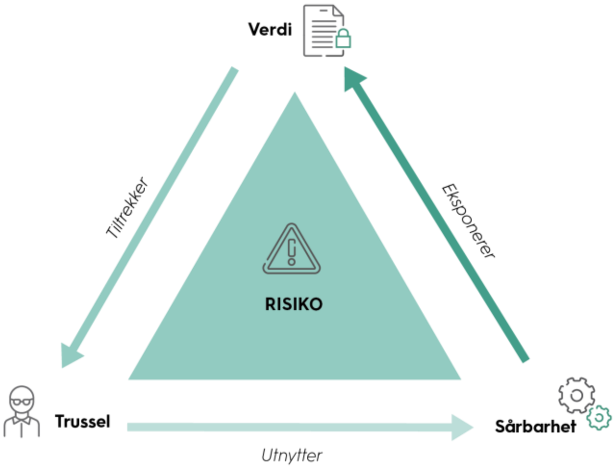

Figure 5: The figure shows the factors that influence information security.

It can thus be argued that without a good overview of threats, vulnerabilities and assets, it will be a very challenging task to identify appropriate measures and barriers. At the same time, an increasing degree of interconnection between systems and solutions, closer links between IT and OT, more automation and an increased degree of digitalisation in general will contribute to more complex value chains which involve multiple actors. There is good reason to assume that more complex and interconnected value chains will increase the level of vulnerability, which is also something that was stated in the Lysne report "Risk management in digital value chains" [2].

On the whole, all actors in the value chain are required to establish good management and control in the area of information security. In the following chapters, we provide an overview of what this entails, including our observations about the status of the actors when concerning these topics.

7 Management and control

A prerequisite for good information security is *management and control*, which, briefly summarised, involve:

- setting targets for the company in line with the expectations of the owners and society
- prioritising, planning, and budgeting the use of resources
- following up and reporting results and use of resources.

It is management that prioritises both short-term and long-term objectives for the company based on the board's expectations and possibly also society's expectations. In order to follow up that these objectives are being achieved, it is necessary to establish mechanisms that provide management with the opportunity to determine whether or not this is occurring. It is these mechanisms that constitute what is often referred to as management and control, or *internal control*. The requirements stipulated in the Management Regulations [3] for internal control and the responsibility related to the follow-up of contractors and suppliers will be particularly relevant for the operating companies.

The purpose of internal control is for managers at all levels to be reasonably confident that the objectives which have been set are being achieved. In other words, all parts of the company are made capable of [4]:

- achieving objectives and performance requirements,
- complying with laws and rules,
- having reliable reporting.

Effective internal control enables company operations to be carried out correctly the first time, and in this way contributes to preventing errors, negative incidents and accidents. The companies thereby achieve the desired quality and efficiency for their products and services. When work processes and tasks are executed in a manner that ensures the desired quality, management can be released from spending time “putting out fires”, troubleshooting and rectification.

Internal control should be integrated into operations as much as possible , i.e. built into existing processes and activities in a manner that ensures structure and quality, even when systems, infrastructure, processes and routines are exposed to adverse effects. This provides a higher level of confidence that the company's activities and tasks will be executed with the expected quality and in accordance with laws and rules and society's expectations. Equinor's "A-Standard Pattern of Action" is an example of where these types of principles are used in operations.

It is important that internal control is adapted to the size of the company and the risks to which it is exposed to ensure that controls and measures are directed to where they are most required. This presupposes that internal control work is risk-based, something which facilitates a cost efficient and expedient balance between resources that are expended on controls and resources used for other tasks.

Risk-based internal control requires managers at different levels to have an adequate overview of risks that fall under their areas of responsibility. In other words, the risks the company should be focussed on identifying, assessing and managing. This enables there to be sufficient confidence that the objectives which have been set will be achieved. This requires structure at operational level. This is where the work of the enterprise is carried out, and where possible deviations and consequences may arise.

8 Risk and risk management

The underlying premise for risk management is that most companies exist to provide value for their owners, and in many contexts also for society. This involves a great deal of uncertainty, and the challenge for management is to determine what level of uncertainty is acceptable in the process of meeting the expectations of the owners and society. Uncertainties represent both risks and opportunities, which can mean losses or gains for the company. Therefore, risk management is about managing these uncertainties, including by steering towards strategic goals and managing the operational risks that may threaten goal attainment in a cost-effective manner. Figure 6 illustrates how risks that are far removed from management's direct influence can threaten the ability of the enterprise to achieve its objectives. Risk management is therefore about managing these uncertainties, including by establishing mechanisms and processes that contribute to managing potentially serious operational risks in a cost-effective manner.

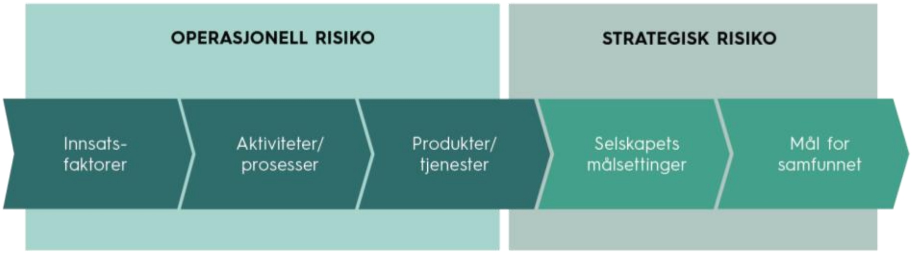

Figure 6: Operational-level risks threaten the enterprise's ability to achieve its objectives.

There needs to be an adequate level of knowledge and quality in the risk management. Regular, qualitative assessments of risk contribute to providing an overview of possible incidents and consequences, an updated understanding of risk, and increased knowledge of the risk picture. Without this knowledge, it is very challenging to determine what measures should or can be initiated in order to get the risk to a satisfactory level.

Good safety work is dependent on the expected safety status being expressed in a clear and understandable manner. This is necessary for the employees to be able to understand what is expected of them and what is sought to be achieved. No one other than the company's owners and management can set this expectation. Such an approach is also supported by both regulations and standardisation; requirement-based safety work gives way to a risk-based approach. An example of this is IEC 62443-3-2. Another example is the Norwegian Security Act and the amendments from the previous Security Act to the new Act, which is more descriptive in its new form. This means that it places greater demands on the company's own ability to identify risks and thereby implement adequate measures to manage these. This is in contrast to normative regulations that go much further in imposing specific measures that may be perceived as unsuitable for the companies and enterprises in question. In order for information security to be proportionately safeguarded in this manner, companies must have internal processes that support it. In other words, a system should exist which ensures that safety assessments are carried out at the operational and tactical level with sufficient knowledge of these processes, and that the assessments are adequately expressed, communicated and understood. IEC 62443, including until now unpublished parts of this series, and ISO 27001, provide a great deal of guidance regarding processes and systems for information security.

As referred to in Chapter 6, information security is about protecting assets associated with information and data against various types of threats that could access these assets by exploiting vulnerabilities within the company. It is an absolute necessity within the petroleum sector to view these assets in relation to potential harm/consequences and criticality. Good risk assessments in the area of information security therefore require that the companies have an overview and control over what and what types of data/information they process and manage and what significance these have in different value chains and systems. There also needs to be awareness of the human, technological and organisational vulnerabilities that exist or may exist, and, finally, it should be possible to conduct assessments of the threat landscape. These factors should then be collated into a comprehensive risk assessment.

There are various methods for doing this, however, regardless of the method used, it is crucial that roles and responsibilities in this work are clarified, and that they are integrated with the overall risk management in the company. This contributes to keeping senior management informed about factors that could potentially threaten the various strategic objectives.

8.1 Information assets

As previously mentioned, all companies in all industries are dependent on different forms of information in their task solving processes. In other words, information has a value, which is often measured by the potential harm if the information or data becomes unavailable, is not correct, or gets into the hands of unauthorised parties. Information is an asset to the company and should be protected accordingly. Assessing this is therefore of major importance to what security measures should be implemented - both logistically and physically. A good overview of these assets and the potential harm to the company and interacting actors if they are lost or compromised in some other manner contributes to better utilisation of scarce resources. In this context, this means that security measures are established where they are required, and that these are dimensioned correctly. In order to determine this potential harm, it is important to first identify the information and then place it in context with other assets. Ownership and classification should also be assigned on the basis of the valuation, which is appropriate in order to be able to provide some information about what requirements the individual asset should be subject to. Within OT, this may involve setting specific safety requirements for the most critical functions, systems, zones, channels or signals. For example, higher criticality may be defined, as referred to in NOG123, and/or a higher Security Level Target may be set, as referenced in IEC 62443-3-2 / -3-3 and NORSOK I-002:2021.

There is ongoing work with IEC 62443-2-2 (the concept of Security Protection Rating, previously called Protection Level) in order to define risk-based requirements for systems in operation. Work is also being carried out to harmonise this concept for operating companies ("Asset Owners") in IEC 62243-2-1 ED2 and in general for this entire series of standards through a new version of 62443-1-1. Several actors in the sector are showing serious interest in these new sub-standards. They are attempting to base some of their work on principles that are available in draft editions of these documents, and which are discussed in various national forums (such as the Sintef CDS forum and NEK NK65). The expected publication date in the IEC for these sub-standards is:

- IEC 62443-1-1 ED2: uncertain, is under development in ISA 99.
- IEC 62443-2-1 ED2: May 2022
- IEC 62443-2-2 ED1: December 2022

8.1.1 Identifying value chains and interdependencies

It is therefore an important prerequisite to have an overview of the assets which are part of the digital value chains that provide various means of support to the enterprise's objective. This is also in line with the National Security Authority's (NSM) fundamental principles for ICT security [5]. As mentioned earlier, operating companies also have a special responsibility in accordance with the Management Regulations.

The degree of complexity and interdependencies in these value chains have a direct impact on the vulnerabilities the company is exposed to. The more dependencies there are, the greater the consequences a single incident can trigger by chain reactions occurring. The more complex the value chains are, the less overview one will be able to assume that one has over the number of actors involved and who is responsible for the system. Incidents in complex value chains can therefore spiral out of control and cause critical processes to grind to a halt. For example, if functions for process monitoring or process control are introduced that are dependent on data or functions in the cloud, there could be major operational disruptions for operating companies and facilities if any of the suppliers of these functions (for example, suppliers of lines, data lakes or SaaS/IaaS solutions) are exposed to DDOS attacks, ransomware viruses or other incidents. There may still be an inadequate understanding of the dependencies of systems and functions and the necessary redundancy may be unclear and uncertain (false redundancy).

8.1.2 Observations and discussion

In order to even be able to assign information a value/classification, it is a requirement that the company has good processes for identifying information elements and their application.

Most of the respondents considered this challenging, however we saw that some have better control over these processes than others. Therefore, the challenge is that there are somewhat different practices for how companies carry out and document valuations of the information that they manage and use. By extension, it is therefore probable that human, technological and organisational security measures are not adequately adapted to the need. In some instances, these will probably be too invasive and costly, while in other instances they are too weak.

There is a relatively large variation in terms of whether or not information is classified among the respondents. This relates to challenges associated with the actual valuation and who it is that carries these out, which in turn is due to it being difficult to link ownership to an evergrowing and complex amount of data and information, and that it can be challenging to understand new technology and new systems. Most respondents have established a good understanding that information ownership should be assigned, however none of the respondents have a clear idea of how this is done well in practice. The responses we received reported that in many cases this is too complex and time-consuming.

We agree that it is complex and time-consuming. At an aggregated level it should not be challenging to link ownership to information, however once models, tables, drawings, etc. are enriched with new information, it becomes more complex. Who owns the database and who owns the various tables, views, relationships, and information objects included within this? These are challenges facing not only the petroleum sector, but is also a classic issue across sectors and something that several different sets of rules are attempting to address.

An example of this is the Norwegian Personal Data Act, which clearly distinguishes between "data controller" and "data processor", where the former can in many ways be equated with the term *information owner*. The *data processor* does as the name implies, i.e. processes data and information on behalf of the data controller. There thus needs to be a set of requirements and criteria that have to be satisfied for such processing to take place. These requirements and criteria follow more or less directly from the regulations, and there needs to be an agreement between the data controller and the data processor, a data processing agreement, in which this is stipulated.

The principles that follow from this should also be able to be applied to information that is not necessarily considered personal data. In other words, the information owner is the party that bears the risk if information or data is compromised, lost or can no longer be trusted. In a value chain, this will probably be the same role, i.e. the party responsible for the results within the area where the information assets and data are most important, or may have the greatest consequences if compromised. It is therefore the process owner who owns the information, because the value chain supports the process. This is in line with the Management Regulations when concerning the responsibility incumbent on the operating company. However, this reasoning does not alter the fact that there may be many process owners (actors, operators) who will be impacted by one element of information being compromised. This is a complex challenge that we know exists, however this report does not respond to it directly. We therefore recommend that the petroleum sector investigates this in more detail in cooperation with academia, other sectors, supervisory bodies (for example, NSM), and government authorities. In our opinion, these investigations should include knowledge and experiences obtained from other sectors, including internationally, that also process data that could have major consequences if it were to be compromised.

Knowledge, principles and experiences should be drawn from IEC 62443-3-2. This provides interesting assessments and arguments for consequence-driven risk assessment, as well as a focus on assessments of worst-case scenarios and the risk to essential functions. Idaho National Lab's model for Consequence-Driven Cyberinformed Engineering (CCE) was also mentioned by some of the respondents and is often raised in various international forums. TR.84.00.09 also refers to consequence-driven risk assessment. Other frameworks that we consider interesting and relevant to obtain knowledge and principles from in connection with risk management and assets include:

- STPA-Sec
- MITRE Mission Assurance Engineering
- Cyber Terrain Mission Mapping

8.2 Vulnerabilities

In a security context, vulnerabilities are the weaknesses that enable a threat or threat actor to compromise the integrity, confidentiality and/or availability of an enterprise's assets. It is therefore important to have knowledge of vulnerabilities in order to identify what weaknesses enable harm to occur. Knowledge of vulnerabilities is essential for being able to view the entire risk picture for both the company and the sector.

There are many different vulnerabilities in digital technology. Some of the most typical for OT and industrial control systems are vulnerabilities related to remote access, incorrectly installed/configured software, use of standard passwords, open protocols, incorrectly installed equipment such as firewalls, ports and services open to the outside, operating systems that do not have the most recent updates, etc.

The various vulnerabilities are normally divided into different categories based on their cause:

- **Human vulnerabilities:** Weaknesses directly related to the person and his/her actions. For example, inadequate knowledge, human errors when processing/analysing data, hastiness and bad habits, limited rationality and cognitive inclinations/bias.

- **Technical and physical vulnerabilities:** Weaknesses related to technology and physical objects. Examples of technical and physical vulnerabilities may include inadequate configuration of accesses, poor network configuration, software errors, open protocols, incorrectly installed equipment, weaknesses in equipment, outdated software, and operating systems that are not up-to-date.

- **Organisational vulnerabilities:** Weaknesses related to the organisation and the enterprise. For example, a poor security culture which enables human error, inadequate knowledge development and awareness, lack of follow-up at management level, lack of guidelines and defined processes for remediation of technical vulnerabilities, weaknesses in access management processes, inadequate organisational insight into assets/vulnerabilities/threats, inadequate background checks of employees from other countries with which we do not have security policy cooperation, fragmented communication and inadequate internal control.

Several of these vulnerabilities, for example, inadequate knowledge, lack of guidelines, inadequate organisational insight into assets/vulnerabilities/threats and inadequate internal control, can result in Open Source Intelligence (OSINT) incidents. This concerns information that threat actors can find in open sources, typically on the internet, and where sharing of information in a situation can reveal vulnerabilities that a threat actor can exploit.

8.2.1 Observations and discussion

A number of suppliers have chosen to publish identified vulnerabilities in their own solutions to their customers, in addition to making this information publicly available. However, this is not the case for all actors. Some do not publish information about vulnerabilities, but rather choose to be more secretive about this and manage it in their own solutions. For those this concerns, this may indicate a weak ability to identify and communicate vulnerabilities. Among other things, this is most probably due to a lack of knowledge about vulnerabilities and the inability to see the importance of knowledge sharing.

Another issue related to vulnerabilities is that it is also not uncommon for rather basic technical vulnerabilities to be identified and communicated, but that the root causes of these are not adequately addressed. There is thus reason to assume that more serious vulnerabilities are not being identified and addressed. Again, this concerns a lack of knowledge, as well as a scarcity of professionals.

Several of the respondents demonstrated that they have an understanding of various vulnerabilities that are relevant to the sector. However, there is a major difference between what the various actors consider to be key vulnerabilities. Among other things, the respondents mentioned the following:

Human weaknesses:

- Inadequate understanding of facilities and processes.
- Inadequate understanding of threat landscape, vulnerabilities and attack vectors.
- Inadequate expertise relating to information security/cybersecurity
- Inadequate knowledge of requirements and guidelines.
- Inadequate knowledge about how to perform work tasks in a secure manner.

Technological weaknesses:

- Access control and problems with having a complete overview of all devices in the infrastructure, value chain issues.
- IoT devices exposed to the internet.
- Inadequate overview and/or control over interfaces/communication channels across networks.
- OT components are not designed to meet requirements for cyber and information security.
- Outdated operating systems in OT components.
- Dependencies on other components.

- Two-factor authentication that is missing or not activated.
- Errors in access management and failure to clean up accesses.
- Inadequate herding of systems.
- Inadequate updating of systems, End-of-Life etc.

Organisational weaknesses:

- Different areas of responsibility within the landscape, not clearly defined areas of responsibilities within cyber and information security.
- Inadequate information security requirements.

OSINT was mentioned in several of the interviews. Some of the sources referred to in the interviews were LinkedIn, Facebook, Shodan, news articles and press releases, VirusTotal (and software uploaded to this website), presentations from conferences and seminars, etc., as well as lists of usernames, passwords, etc. from digital break-ins.

Most of the respondents were aware of sensitive information about their activities having inadvertently been made available in open sources. The companies take reactive measures to remove this information, and the majority of them also appear to have proactive processes for preventing the inadvertent sharing of sensitive information to open sources. There are awareness campaigns and information in open sources is identified, and some companies also carry out surveys on the dark web. However, the respondents reported that it can be challenging to assess the extent to which information regarding vulnerabilities can be derived from the growing amount of company-specific information that is available in open sources. In most cases, usernames, passwords, and IP addresses are considered information that must be treated confidentially. There are discussions as to whether topology drawings, Slowly Changing Dimension (SCD) and Piping and Instrumentation Diagram (P&ID) etc. should be handled confidentially, however there is no consensus on this. For example, this discussion includes challenges relating to ensuring that what is now non-sensitive information could potentially be considered sensitive information in the future, and that strict management of information sharing creates challenges in relation to collaboration, knowledge development and achievement of results for the companies and the sector as a whole.

The interviews also revealed that the actors use different methods for detecting vulnerabilities. These range from reactive/ad-hoc to more proactive and systematic. For the human vulnerabilities, there is often internal training and testing of phishing attacks, follow-up and assessments/investigations following undesirable incidents. One company reported that it conducts annual exercises relating to serious incidents in which the entire emergency response apparatus is involved, as well as exercises at individual facilities. In terms of organisational vulnerabilities, it was reported that external and internal assessments and risk assessments are used and that an information security management system (ISMS) is established. For those who already have a management system, this is updated and followed up. For technical vulnerabilities, strategies include scanning to identify vulnerabilities at endpoints, various forms of testing, such as code testing and review, and penetration testing. Various sensors are also used to detect technical vulnerabilities in digital infrastructure. Further information about technical vulnerabilities is obtained from, among other things, the National Cyber Security Centre (NCSC) and KraftCERT.

In terms of the human vulnerabilities, it was reported that different parties are involved in detecting and gaining an insight into these. Training materials are prepared by the specialist groups and management is responsible for ensuring that employees have sufficient expertise and knowledge. For technical vulnerabilities, security teams, operations service providers, specialist cyber and information security groups and risk owners are used to detect these vulnerabilities. It was reported that those involved in the organisational measures are often specialists within the field or owners of processes and requirements.

On the whole, the respondents reported many relevant and key vulnerabilities within cyber and information security. However, we are still left with the impression that the vulnerabilities are often citations from the textbooks and that there may be a lack of good expertise in this area, and particularly within some of the vulnerability categories. It was also clearly stated by all of the respondents that the primary focus is on the technical vulnerabilities in digital systems. It appears to be this category of vulnerabilities that the majority have the greatest knowledge about, both in terms of what vulnerabilities they consider to be key vulnerabilities and methods used to detect such vulnerabilities. There is generally little focus on human and organisational vulnerabilities. We also find that there is not enough focus on non-digital technical vulnerabilities that should be viewed in connection with digital vulnerabilities. By this we mean, for example, weaknesses or limitations in construction dimensioning, design/philosophy in process control and safety systems and potential errors in Cause & Effect logic. This is an indication that there may be a lack of expertise and awareness in the sector. Long value chains, complex systems and uncertainty relating to independence between barriers also paint a more confusing picture of relevant vulnerabilities.

A clear picture of the systems and architecture is required in order to identify the assets and vulnerabilities that threat actors can exploit. Without an adequate enough overview of, and expertise in, key vulnerabilities and chains of vulnerabilities, as well as an established responsibility for following up and managing the vulnerabilities, it is difficult to view the entire risk picture.

Several of the actors would have benefited from detecting, communicating and managing vulnerabilities if they had had access to a more unified industry standard. The Regulations, NoG documents, NORSOK standards and NSM's Basic Principles for ICT Security do not adequately cover this at present. In our opinion, IEC 62443 and DNV-GL-RP-G108 provide good supporting documentation for being able to create a more uniform industry standard moving forward.

It would also be of benefit if the oil and gas sector had a clearer common platform or channel for being able to share information and knowledge about vulnerabilities, for example, KraftCERT. It is of particular importance that information about vulnerabilities is shared with each other in the value chain. A vulnerability located far up or far down the value chain can have equally serious, if not more serious, consequences at the other end of the chain if the vulnerability remains undetected and is not managed or communicated over an extended period. The attack on SolarWinds is a good example of this. For a more detailed description of the SolarWinds incident, see Appendix 1.

8.3 Threats

Defining the threat landscape within information and cybersecurity is not a simple mathematical exercise. Many attempt to quantify risk by putting a figure on the consequence and probability associated with an undesired incident. Such quantification can be useful in connection with comparisons with acceptance criteria and prioritising risks for which measures must be taken. However, a quantified picture of risk provides a rather simplified representation of the risk picture. Precision in numbers may also give the impression that the threat landscape is adequately understood, while the risk may, in reality, span a wide range, be linked to a high level of uncertainty and/or be based on very deficient data, little historical data or weak knowledge/expertise. The petroleum sector faces major challenges in obtaining an overview of weaknesses, dependencies and potential harm, and there are thus many qualitative aspects that cannot be converted into figures with an adequate level of precision or that are suitable for communicating risk in an understandable manner. In order to understand the threat landscape, it may therefore be appropriate to look at relevant incidents and attacks, both intended and unintended, and use this to garner an image of what was possible in the past, what is possible now, and what may be possible in the future.

The industry faces a complex threat landscape. Applicable threats to the petroleum sector may be technologically advanced, and the threat actors may possess considerable resources due to them sometimes being supported by entire nation states. Their motivations can be very different and can range from groups that want to cause the sector to suffer financial and reputational loss, to advanced actors who are working to profit from military and/or industrial espionage, and perhaps only want to position themselves for a future situation of greater geopolitical unrest. This threat landscape also applies across sectors and industries. Threat actors for industrial control systems can also be everything from individual attackers and activists to organised criminal groups or terror-related groups.

8.3.1 Intended and unintended incidents

Deceptive and intentional incidents involving malicious actors further complicate assessments of the threat landscape. A deceptive, malicious actor may be able to exploit weaknesses in people, technology and organisations across systems, and may also be able to create new weaknesses through their systematic and targeted actions. It can be impossible to predict the actions that a threat actor may carry out. Historical incidents and frequency can indicate trends and developments, however will not be able to be used precisely to determine who will be attacked, how the attack will be carried out, where it will occur, how often it occurs or what the threat actor is on the hunt for. Examples of intended incidents for which we are seeing an upward trend and increase in frequency are ransomware viruses, supply chain attacks, and ransom-DDoS ("rDDoS") attacks. There are also unintended incidents that can occur both through human error and natural events. Some examples of relevant incidents and attacks are listed below. For a more detailed description of these incidents, see Appendix 1.

- **Triton/TRISIS** was an advanced, complex and deliberate attack in 2017 that made changes to/sabotaged safety instrumented systems (SIS).
- **Ekans** was a ransomware virus that was detected in 2019 and which had ICS-specific objectives and capabilities for stopping ICS processes.
- **Colonial pipeline,** one of the USA's largest pipeline systems for transporting refined oil products, was exposed to a ransomware virus in 2021 that resulted in massive disruptions to their distribution.
- **Telenor** was hit by a Ransom DDoS attack in 2020 that demanded ransom money to not subject them to further attacks.
- **SolarWinds** was the target of a supply chain attack in 2020. Several major actors use the service that they provide (Orion), including the United States Department of the Treasury, Microsoft, as well as several customers in Norway, including in the petroleum sector. Hundreds of companies across large parts of the world were subjected to this indirect attack.
- **Kaseya** was the victim of a supply chain attack in 2021 that impacted, among others, Coop in Sweden and resulted in them having to close several of their stores for a period of time.
- **The Mongstad Refinery** experienced an unintended incident in 2014 that resulted in them having to shift to manual loading and a loss of NOK 200,000-300,000 for Equinor (formerly Statoil).

8.3.2 Open threat assessments for 2021

Each year, Norway's intelligence and security services publish their open threat assessments. Below we have collated the most important elements from each of these for 2021.

In their threat assessment for 2021, the Norwegian Police Security Service (PST) placed most emphasis on three threats: state intelligence activities, politically motivated violence and threats against government officials. State intelligence activities are the type of threats that stand out for the petroleum sector. The motivation is to collect information and influence decision-making. It is expected that foreign intelligence services will carry out assessments of Norwegian infrastructure, as well as recruit sources. Specific reference is made to the fact that enterprises within the petroleum sector should be prepared for attempts to steal information. There is also an interest in physical and digital smart city solutions that can provide a detailed overview of Norway's critical infrastructure. Acquisitions and investments in the business sector, exploitation of academia for illegal knowledge transfers, and surveillance of dissidents and refugees who are in Norway are listed. [6]

In the Norwegian National Security Authority's (NSM) report entitled "National digital risk picture 2021", the NSM describes the types of digital incidents that impact Norwegian enterprises and the consequences these have for joint digital security. The report highlights the problem of long value and supply chains that make it more difficult to keep track of the vulnerabilities that can be exploited by threat actors through, among other things, supply chain attacks. The NSM notes that in order to withstand undesired digital incidents, the implementation of technical measures alone is not sufficient, but together with human and procedural measures will help to reduce the risk. Digital security is a management responsibility where the enterprise and management are always responsible for protecting their own assets, and where risk assessments and risk management are crucial for achieving an acceptable level of security in the enterprise. The NSM also highlights the importance of transparency around incidents and information sharing because this leads to greater general awareness in society. [7]

In their "Focus 2021" report, the Norwegian Intelligence Service (NIS) placed emphasis on great power rivalry, terrorism and digital threats. The NIS wrote that "foreign intelligence and influence activities remain a significant threat to Norway and Norwegian interests." The primary threat in the digital space is espionage from state actors. In connection with the digital threats mentioned in the report, the NIS wrote that network operations are used both for intelligence and destructive operations such as sabotage. In addition to this are influence operations which have the objective of influencing elections and political processes and of spreading disinformation. Intelligence operations to extract information take place within the defence sector, in security and foreign policy, and in the health and energy sectors. Actors in Norwegian industry that manage information within, among others, the Norwegian energy, oil and gas sectors, are mentioned as being targets for Russian actors. [8]

8.3.3 Observations and discussion

The sector is partly conscious and aware of the described threats and incidents. However, we cannot draw the conclusion that strategic and operational choices are based on this awareness and that the knowledge is adequately applied to protect industrial control systems and associated data at rest and in transit. It is clear from a business economics standpoint that industrial espionage could have serious financial consequences. Similarly, state intelligence activities in the sector may inflict serious losses on society that will not necessarily be visible in the companies' balance sheets and income statements in the short term. Nevertheless, it does not appear as if the actors have good enough mechanisms for management, internal control and internal communication for adequately detecting and preventing such threats. There is even less focus on the potential for sabotage and terrorist attacks using digital technology. Among other things, this applies to supplier arrangements, access management and rights, classification of information and assets, lack of control over value chains and inadequate change control over digital value chains and solutions. The impression given is that a threat landscape involving foreign and state threat actors would be too vast and complex for these enterprises. At the same time, it is argued that there is a low probability of such threats occurring. We question this argument based on the trends we are seeing internationally, the incidents we are seeing ourselves, what we informally gain an insight into, as well as the fact that probability assessments for cyberattacks are a very difficult and complex task that even the best intelligence agencies appear to have challenges with.

On the whole, this is an indication of a lack of knowledge and scarcity of professionals in this field. In their open threat assessments for 2021, both the Norwegian Police Security Service and Norwegian Intelligence Service stated that we will see increasingly more of foreign and state actors in the years ahead. It is therefore important that the enterprises are aware of these and possess sufficient knowledge and expertise for being able to manage and protect themselves from these key threat actors. Therefore, as was also noted in the NSM's report for "National Digital Risk Picture 2021", it is not good enough to only implement multiple technical measures. The enterprises must also have the human and organisational measures in place to reduce the risks posed by the threat actors. In order for digitalisation and an increased level of automation to produce the expected benefits that form the basis for the strategic choices made by the actors, knowledge and awareness of these topics, and good management and control of the information security work are required.

Both intended and unintended incidents can be avoided to a greater extent through sufficient knowledge of threats and the overall threat landscape. In addition, continual work on identifying threats is vital for reducing the risks associated with incidents. An important factor for succeeding in this work is effective communication and being more transparent about threats and vulnerabilities across the sector, across multiple sectors and between companies and government authorities.

However, this appears to be a relatively major challenge at the present time. Several respondents noted that it is difficult to find good information about vulnerabilities and threats for OT. This applies to the energy, oil and gas sectors in general and for industrial control systems. Despite several of the interviewees having partnerships, subscriptions or acquiring information about the threat landscape and incidents through, among others, the NSM, KraftCERT and NCSC, this does not provide enough information, because much of the information concerning incidents and vulnerabilities is only shared to a limited extent or is confidential or classified. Furthermore, information concerning incidents is often complex and has some uncertainty. It is therefore challenging to communicate this in a manner that is clear, unanimous and comprehensible. Even though the message appears clear on the part of the sender, it does not need to be understood correctly by the recipient. Therefore, major communication challenges arise internally within the companies, between the companies, across sectors, and with government authorities. With regard to the DIKW model referred to in Chapter 4, data therefore does not become good information, and neither knowledge nor wisdom is created.

We see the same communication challenge in terms of the threat landscape, vulnerabilities and assets and in terms of potential consequences. The companies have different specialist groups, perspectives and opinions, and in some cases communication between them takes place through formal communication lines. While travelling through these channels and transport stages, it is probable that the information will become unclear, uncertain, deficient, incomplete and misunderstood. This may be because information is not communicated between actors, that errors arise in the information being exchanged, that not all information is transferred, or that the information provided is misunderstood by the recipient [9]. One is therefore left with information that, in isolation, does not improve one's understanding and the basis for making decisions thereby becomes inadequate. This communication gap is clearly seen between IT experts on the one hand and OT/automation experts on the other. They are often in different business areas, and therefore many organisational links removed from each other. The IT people possesses a great deal of knowledge about vulnerabilities in digital systems and the threat landscape, while the OT people know a lot about the physical potential for consequences. In terms of knowledge about vulnerabilities, the threat landscape and consequences, they stand at opposite sides of the enterprise, each with their own "tribal language", with inadequate, fragmented information, and they have major challenges in combining their common data/information into knowledge and wisdom for the enterprise.

9 Information Security Management System (ISMS)

Information security is just one of many areas that require management and control. As mentioned earlier in this report, this is about establishing structures and processes that enable the companies to identify information and data, assess vulnerabilities, and be able to obtain an overview of what threats may be applicable at any given time. The companies and organisations that work systematically with information security, including those that work risk-based, are better able to implement cost-effective measures where these are required to prevent undesired incidents, or to reduce the scope and consequences of such incidents. The benefits are better management of incidents and faster recovery to a normal state if things first go wrong. Good safety work must therefore be cost-effective. This requires management, and good management entails that:

- roles and responsibilities in the organisation are defined, clarified and clearly understood,
- processes for risk management are established and that the correct roles assess and manage identified risk in line with adopted criteria,
- there are mechanisms which ensure follow-up and control that safety requirements are being complied with

A systematic and risk-based approach to information security normally requires an information security management system (ISMS). An ISMS is to information security what a quality system is to the company's other products and services, i.e. a framework that describes the minimum requirements for the company's work with information security. This framework should be entrenched in senior management and administered by an information security manager or equivalent role. The framework and requirements for operating companies must also be in line with the additional responsibility that is assigned to them through the Management Regulations. By setting overarching requirements in a number of areas that impact horizontal and vertical work processes and activities, the company will be able to detect and prevent information security incidents, as well as more quickly restore to a normal state if incidents first occur. The overriding objective is always to be able to protect the information assets such that the requirements for integrity, confidentiality and availability are identified, balanced and safeguarded.

Without structure and internal control, few enterprises will be able to obtain an overview of all value chains and processes that different information passes through and influences. There will be even less oversight over organisational, human and technological vulnerabilities. A lack of structure, risk management and control mean that development projects and other digitalisation initiatives also do not support and safeguard the actual business requirements. In other words, there is a high risk that the benefits will not be realised.

A management system for information security that is based on recognised standards such as NS-ISO/IEC 27001 is an important instrument for being able to achieve such management and control.

9.1 Organisation of safety work

Another important component in all internal control work, including in the area of information security, is organisation. It can be argued that without satisfactory organisation, it is also not possible to establish adequate internal control. This means that there are clear frameworks for which roles have decision-making authority for what, and that this is particularly viewed in the context of who owns risk.

It is always the chairman of the board of directors who has primary responsibility for the company's results. This responsibility is normally delegated to a managing director, who ensures, on behalf of the board of directors, that the company achieves the results that the owners expect. It is therefore the managing director who is primarily delegated the company's risks, however it is not appropriate for all decisions go via the senior manager. This is generally resolved by delegating different parts of the company's overall risk portfolio down the line to the roles designated as performance managers in their areas. These roles own the information that supports the business processes for which they are responsible. At the same time, it is not necessarily the case that each performance manager has sufficient expertise or insight to set adequate information security requirements, nor that these are in line with senior management's requirements and expectations. Therefore, this requirement should be based on a staff function or the equivalent, which is not unlike the manner in which most actors in the oil industry organise their HSE work.

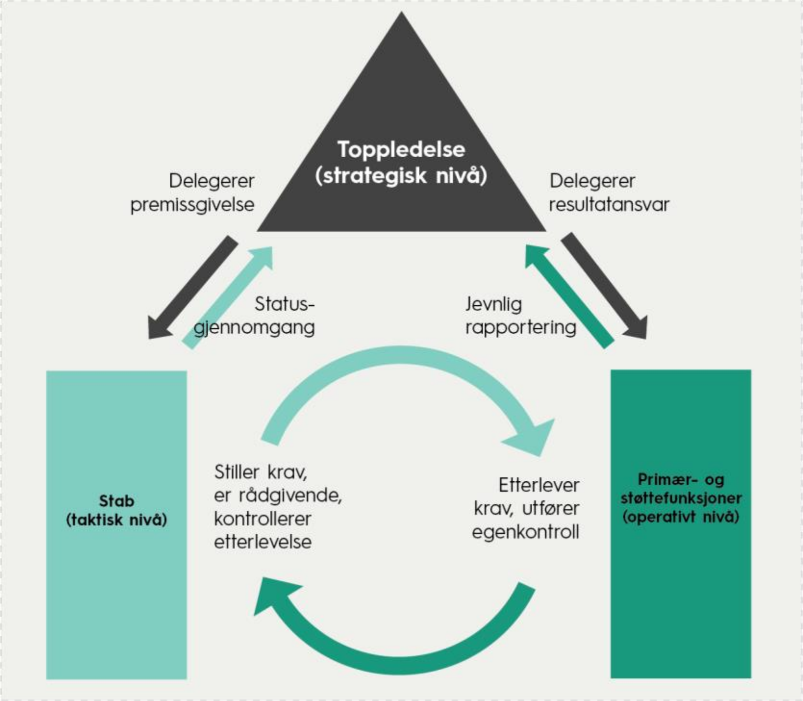

Figure 7: Separation of roles, the responsibilities of the roles and the relationship between them.

This requirement should be delegated to someone with a good level of expertise within security, business and internal control, who formulates the premise by supporting and following up the security work, and having a close dialogue with senior management about the level of risk. This role is normally a chief information security manager or CISO. Senior management should be clear in their communication that the role of the CISO is to establish and express security requirements on their behalf, and that these are the CISO's most important tasks, as well as following up that the security status is in line with management's expectations.

In any case, the crucial element is to ensure the separation of roles, i.e. that there is a distinction between the requirements specifier and those who perform the day-to-day operations as shown in Figure 7. These principles are equally as valid in information security as they are in other internal control areas, and this form of separation of roles contributes to management achieving two things:

- regular status from the line through regular risk reporting, which can be compared with
- periodic and impartial status from the premise provider.

Such organisation reduces the probability of requirements specifiers ending up in unfortunate dual roles. The role is thus cultivated as premise setting, controlling and advisory. The performance managers, i.e. those who own risk and information, will for their part be able to concentrate on adapting and adjusting processes and activities in order to reduce vulnerabilities as best as possible in line with the commercial needs and requirements that may otherwise be dictated by the management system.

IT knows IT best, and IT is measured in relation to IT. By organising the premise-setting for information security in the IT organisation *there may* be incentives to play down potential concerns related to, for example, cultural challenges and compliance in the organisation, and instead highlight the importance of even more technical security measures. This can degenerate in various forms, such as downgrades of risk assessments and embellishing reporting to senior management. This version of reality then results in senior management “flying blind” by not being made aware of the actual risk level and not being able to place information security on the agenda until an external authority discovers anomalies and regulatory breaches, or that the enterprise is shown to be compromised. However, by then it is too late.

The same mechanisms and challenges may apply if the premise-setting is organised in OT.

9.2 Observations and discussion

Our sample reveals that most respondents work in a structured manner with information security, i.e. that they have, at a minimum, established governing documents that are entrenched with senior management. With regard to the extent to which these are implemented, i.e. whether information security is integrated into processes and activities in general, such as in overall HSE work and internal control, we see greater variation.

Some are certified in accordance with ISO 27001, some are in the process of implementing the standard in their overarching internal control systems and day-to-day work processes, several work according to the standard, while others are neither certified nor working in accordance with ISO 27001. A positive finding from the interviews is that a larger proportion have established structures that ensure internal control in the area of information security than the proportion who have not. It is also positive that more understand the significance and importance of integrating management and control in the information security area as much as possible with the other internal control work. In our view, this alone is a sign that there is a high level of awareness among both managers and employees. One of the companies in the sample, a supplier company, surprised us in a very positive manner with their mindset and maturity in managing information security. We are of the opinion that, in the long term, this will bear fruit in projects and solutions that this company is involved in. Such continuous, process-based improvement, which in COBIT is defined as "leading indicators", will outperform ad-hoc sprint races. Similarly, Equinor's "A-Standard Action Pattern", with a learning loop, can increase the quality of deliveries over time.

When asked who it is at the companies that determines acceptance of risk, most actors responded that it is either directly or indirectly the senior management who is responsible for this. The companies we consider to be the most mature have this formalised through policies or other overarching governing documents. These are approved and signed by senior management. Our findings otherwise indicate that most of the actors have established mechanisms to ensure that management in the respective companies are kept informed about the risk picture. The vast majority responded that they carry out risk assessments when this is necessary and that processes have been established which ensure that the security requirements are also reflected in contracts and agreements.

However, we question the extent to which the responses reflect the realities. As has already been discussed in chapters 4 and 8.1, there are rather different answers when concerning, among other things, identifying information assets and the people in the various companies who are responsible for these. We consider it challenging to achieve adequate risk management if the company does not have an overview of its information assets. It will also be a challenge if it is not possible to link ownership to these. Some of the respondents also appear to be somewhat uncertain about the meaning of the term "risk owner", i.e. what this entails.

The responses were also vague when concerning communication and possible management of risk between the actors in the value chains. This is understandable, because it is more challenging and complicated to establish good risk management that involves multiple actors with different interests. This can be resolved by the client expressing its willingness to take risks through clear and precise requirements for, among other things, information security in agreements and contracts, and that good processes are established for following up the suppliers. This requires good procurement expertise. IEC 62443-2-1 ED2 and IEC 62443-2-2 ED1 are of great interest in this context.

However, it is our understanding of the suppliers in particular that it is not always the case that there is good procurement expertise. Several respondents stated that operators often accept deliveries that are "inferior" to what is stipulated in the contract, and that this is only adequately handled afterwards. The reason given for this was that the operators are not as professional in terms of the IT aspects for procurements as they are in other situations, i.e. this may indicate a lack of procurement expertise when concerning IT or complex digital technology. In any case, this is an interesting observation, since it is, in isolation, an indication that information security is both considered an IT matter and/or that it is not perceived as particularly business critical. This is otherwise supported by those who participated in the interviews. With some exceptions, the respondents largely represented IT in the various companies, and it was in many ways challenging to gain an insight into how internal control and risk management take place at an enterprise-wide level, including how this is organised.

On the whole, our assessment is that most of the actors we spoke to, including both operators and suppliers, have a basic understanding of information security. However, this is very strongly linked to IT, and thus information security will become too far removed from the core tasks due to it being perceived as a responsibility that IT has to deal with. This approach may work in some situations, however IT should not take the risk on behalf of the process/risk owner as this is what it most probably will be. We consider this to be precisely the case with the majority of the respondents we have spoken to. The result may be that the risk owner and the companies are exposed to greater than acceptable risk, and this is continued further into contracts and agreements – something that can expose the client to an even greater extent.

10 Knowledge

In order to maintain a satisfactory level of security, it is essential that all employees have sufficient knowledge of information security and IT security. This is particularly important when digital developments are occurring at a record pace. As referred to in this report, many incidents, both intended and unintended, can be attributed to employees having inadequate or no security expertise. Threat actors manipulate employees to gain unauthorized access to systems and infrastructure, or employees perform actions they should not be performing due to a lack of knowledge. Both contribute to data and information being compromised.

The competence and knowledge of the individual employees is important, however in the larger picture it is a good safety culture at the enterprise that is of key importance to ensuring that measures that have been decided to be implemented are followed and complied with. As shown in Figure 8, organisational culture is influenced by knowledge, awareness and skills. Knowledge contributes to the satisfactory performance of work tasks, while awareness contributes to reinforcing or changing behaviours and attitudes, as well as encouraging compliance with the enterprise's values. Skills are also necessary for being able to act correctly and influence the enterprise in a positive manner.

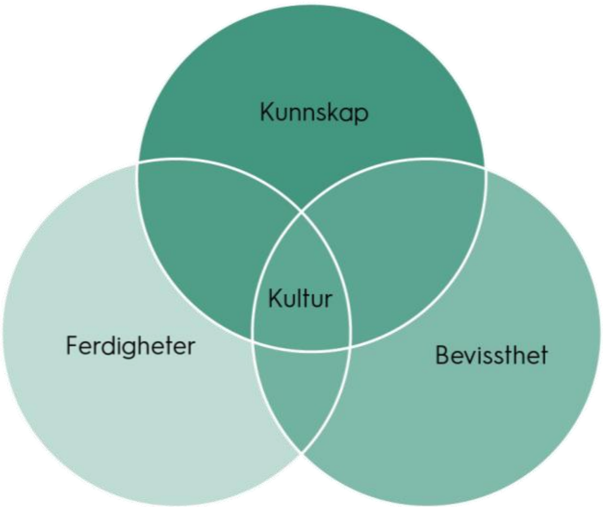

Figure 8: Knowledge, awareness and skills are important factors for having a good security culture at the enterprise.

There are various methods for building knowledge, awareness and skills. According to leading practice [10] [11], all employees at the organisation, and contractors when relevant, should receive education and training to build knowledge, awareness and skills. Among other things, these activities should be based on experience from previous security breaches.

To build knowledge, awareness and skills, it is important to focus on "why", in addition to "what" and "how". A good knowledge base contributes to increased awareness of the following:

- **What does it mean for me?** It is important that all employees have awareness and knowledge of what constitutes security and what it means for themselves and their own enterprise. Employees need to understand the purpose of information security and the potential positive and negative consequences their own actions may have for the enterprise.

- **Why is it important?** Employees need to have an understanding of why each individual must maintain information security, including the importance of this.
- **How can I best comply with our internal requirements?** Each individual must also have an understanding of the responsibility that one has as an employee in order for the enterprise to comply with adopted instructions and governing documents.

10.1 Observations and discussion

There is a varied level of focus on training and knowledge development among the respondents. Some have more formalised arrangements than others. It appears that all respondents offer varying degrees of training for their employees, especially for new employees, and several conduct different courses. However, the extent to which the training focuses on security varies.

Some focus more on physical safety in the training, while others emphasise information security and IT security. Some actors use training tools such as NanoLearning and PluralSight, while others train their employees through both internal and external courses. Some of the training is geared towards ISO 27001 when this is used, while at the same time, not much of the training is focussed on the IEC 62443 standard or industrial cybersecurity. One recommendation would be to include more security and more areas of security in the training carried out by the various actors, specifically training that focusses on IEC 62443/industrial cybersecurity. There are several alternatives for training employees. This can take the form of classroom-based teaching, lectures, e-learning, exercises, dilemma training, "train the trainer", etc. It is essential that the training materials and initiatives are considered relevant to those concerned, based on their roles, responsibilities and skill level. It is therefore recommended that target groups are identified and prioritised in order for the knowledge-enhancing activities to have a positive effect on the individual employees. The materials should also be relevant to the sector, something that can be achieved by using examples of applicable vulnerabilities, assets, threats and incidents from the industrial and petroleum sectors.

Experience from attitude-creating work in a number of organisations indicates that e-learning courses are an effective means of reaching out to all employees. e-learning is a measure that can be used to raise awareness of areas in which it is important that all employees are familiar with, such as reporting deviations, secure processing of information, passwords and social manipulation. Complex materials, which need to be further refined in order to be understood and internalised, are not suitable for e-learning. This means that e-learning which relates to information security will not in itself be sufficient for reaching out to all personnel and all roles.

It was reported that awareness-raising activities preferably take place through brochures, campaigns, phishing tests, exercises and the sharing of information via internal channels such as Yammer, WorkPlace and Teams. Several also use the annual security month in October as an arena for improving the security culture by raising awareness.

One of the suppliers reported that they have an ongoing “Security Awareness Program” which includes weekly internal communication, presentations at staff meetings, threat modelling and both digital and physical courses for employees. This supplier also looks at experiences they have had in connection with incident management and this information is shared across the enterprise. It was reported that one of the operators has carried out attitude-creating activities in the form of phishing tests that were sent out to both internal employees and suppliers.

All of the actors also acquire knowledge about incidents and preventive security work through partnerships with, among others, the NSM and KraftCERT, as well as through their participation in security forums, for example, Norwegian Oil and Gas and CDS forum. This enables knowledge to be shared across fields of expertise, service routes, companies and roles. Several respondents reported how initiatives from KraftCERT are starting to become good forums that contribute to communication and knowledge development. In connection with this, mention was also made of Sintef PDS/CDS forum, NCSC's IRC channel, OT forum, committees, conferences/seminars/courses and that employees are permitted to use working hours for knowledge development and participating in such forums. Participation in relevant forums, as well as partnerships with, among others, the NSM and KraftCERT, help to improve knowledge and raise awareness about relevant incidents and possible vulnerabilities. However, as previously mentioned, this information is fragmented, because information pertaining to vulnerabilities and incidents is often classified or treated confidentially, which means that much of the important information is not available to most actors in the petroleum sector. The impression is otherwise given that there is *insufficient* knowledge sharing when concerning incidents, threats and other relevant and good security-related information across the companies. It is barely scratching the surface. This is also the impression we are left with after a great deal of work across companies. We also see an absence of knowledge sharing in several other sectors, as well as between sectors. Several respondents reported that it is difficult to obtain a good overview of vulnerabilities, threats and the probability of incidents and attacks, and that increased knowledge sharing across companies and sectors is necessary.

One of the companies, which we found to have some focus on training and providing courses for employees and managers, reported that performance indicators are not currently used to determine if this training is having an effect. One of the supplier companies that uses Pluralsight as a training platform utilises Pluralsight's built-in tools to measure employee skills. We have been informed that these compare the results before and after training has been completed. Among other things, the supplier in question has used this method for security training in connection with Azure.

On the whole, the impression is given that only a few of the actors have an established quantification process that looks at the situation before and after competence raising measures have been implemented. It is therefore difficult to determine whether the teaching, awareness activities and training have a positive impact on the employees. Without performance measurements, it will be very challenging, not to say impossible, to be able to provide a concrete answer to whether the training functions as intended, and whether the actors thus achieve the desired results. We therefore recommend evaluating the effect of the activities that are carried out in connection with the development of knowledge, awareness and skills. This will require the companies to define learning objectives adapted to the enterprise and to use these as a yardstick.

11 Conclusions and recommendations.

The petroleum sector is continually exposed to various types of risk. If we assume that the respondents are representative of the sector, we are doubtful that the sector is able to adequately identify and manage the risks associated with information security. When viewed in connection with the fact that information security is not being sufficiently taken into consideration in supplier management, our conclusion is that information and data are not being adequately protected, either while in transit or at rest.

There is a great deal to suggest that the operators are not aware of the risks they are exposed to, partly because the threat landscape is both unclear and to some extent ignored when it becomes clearer, and that there are no good processes for being able to identify and assess internal vulnerabilities, particularly those of an organisational and human nature. Furthermore, based on the organisational vulnerabilities being present to the extent that we have seen, including weaknesses in the organisation of security work, risk management and training, the work of detecting and managing risk is reactive and to a lesser extent planned. In our opinion, it is therefore overwhelmingly probable that threat actors with sufficient capacity and motivation have already compromised infrastructure and systems.

Our observations and findings indicate that there is a great deal of information and data that very few actors in the value chains have a good enough overview of, and there are thus no specific assessments of the potential consequences if this information and data are compromised. Most have an idea that there may be consequences, however, because ownership has not been clarified, a vacuum exists that allows new solutions and IT systems to be linked to existing infrastructure without operators necessarily having sufficient knowledge or control of this. Therefore, information and data flow between systems and solutions without the necessary measures being implemented. The suppliers make their assessments, but this is done piecemeal and divided without a larger whole or without the correct roles at the operators being sufficiently involved. As discussed earlier in the report, there are many potential consequences, and the ramifications of this could span across many more dimensions than simply pure financial costs. Society can also be harmed.

We attribute this to several factors we have explained in this report:

- Inadequate management and control of information security on the part of both operators and suppliers, particularly in complex value chains.
- Inadequate focus on information security in supplier management and follow-up.
- Inadequate knowledge, competence and awareness of threats, assets and vulnerabilities.
- Insufficient exchange of both threat information and information about vulnerabilities between government authorities and the industry, as well as internally in the industry.
- Vulnerabilities are often addressed by implementing new technical solutions, which in many instances can further complicate value chains, rather than working systematically

with awareness-raising and knowledge building, or properly addressing larger organisational challenges.

When strengthening knowledge development, care should be exercised with the duty of notification. We see that requirements and regulations for whistleblowing can be counterproductive because there are often elements of uncertainty relating to incidents and risks, they create internal and external disruptions, and can conflict with production targets and performance requirements. Our experience is that this results in underreporting, inadequate communication and an unwillingness to conduct analyses or investigations when formal requirements are attached to whistleblowing in areas that are often confidential. On the other hand, we see that knowledge exchange and information sharing take place more efficiently on informal forums.

It is our understanding that the Petroleum Safety Authority Norway uses ISO 19011 as a basis for its supervisory methodology. We have registered that some actors consider themselves to be more of a target than others for such supervision, which in itself does not have to be wrong. However, this may be a sign that more emphasis is placed on the perceived importance than the objective inherent risk when supervision is planned. At the same time, we have been made aware that the supervision inadequately identifies the instances in which management systems and internal control do not function in the manner in which they are often presented by the companies. There may be various reasons for this, however a traditional audit approach is normally required to detect this, for example, through so-called system testing (check/testing of the companies' controls/internal control) and substance controls based on statistical samples. This also contributes to making the audits more efficient and that the number of audits can be increased without correspondingly increasing the use of resources.

11.1 Recommendations

- The companies should increase their efforts to integrate existing internal controls in the security field into the companies' overall internal control, including that processes for risk management and supplier follow-up are covered by security requirements.
- The companies should ensure that the importance and responsibilities of different roles are viewed equally within the company and throughout the entire value chain.
- The companies should, to a greater extent than at present, conduct assessments of the significance that loss of confidentiality, integrity and availability have in relation to the processes and value chains that are supported by different data and information. The potential for consequences must be thoroughly assessed and at an interdisciplinary level.
- All actors should link ownership to information and data to a greater extent. The operating companies in particular have a responsibility in relation to, among other things, the Management Regulations, to set the contractors and subcontractors requirements for this.
- Efforts should be made to reach an agreement on what mechanisms have to be used to protect data and information that are at rest.

- Stronger and clearer requirements should be set for the implementation of access management functions at endpoints which restrict what assets can be changed and what access should generally be granted to. This includes moving away from privileged access, with rights that exceed what is necessary.
- Consideration should be given to adopting more modern, dedicated tools for change and version management in OT.
- The companies should review the organisation of the information security work, including ensuring a greater degree of role separation.
- Efforts should also be made to include more security, especially IEC 62443/ industrial cybersecurity, in the training conducted by the various actors. In connection with this, it is essential that the teaching materials and initiatives are considered relevant.
- The effect of training activities should be better able to be quantified and subject to evaluation.
- More informal forums and meeting places should be established to develop knowledge about incidents, vulnerabilities, threats and assets across specialist groups, companies, sectors and government authorities.
- The Petroleum Safety Authority Norway can assume a more prominent role when communicating with the actors. The project found that some respondents expressed a desire for clearer management signals, particularly when establishing relevant standards and regulations.
- The Petroleum Safety Authority Norway may seek to achieve a more risk-based approach when conducting supervisory activities by adopting traditional audit methodology insofar as this is appropriate. In this context, our assessments and recommendations are consistent with the DNV GL report "ICT security – Robustness in the Petroleum Sector, Regulatory and supervisory methodology".

12 References

[1] S. Pedersen, "Vær et A-standard menneske!," *BIS Magasinet,* pp. 22-23, 2012.

[2] O. Lysne, "Risikostyring i digitale verdikjeder," Direktoratet for samfunnssikkerhet og beredskao (DSB), 2020.

[3] Lovdata, Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (styringsforskriften), Helse- og omsorgsdepartementet, Klima- og miljødepatementet, Arbeids- og sosialdepartementet, 2011.

[4] M. E. Everson, S. E. Soske, F. J. Martens, C. M. Beston, C. E. Harris, J. A. Garcia, C. I. Jourdan, J. A. Posklensky and S. J. Perraglia, "Internal Control- Integrated Framework," COSO, 2013.

[5] "NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0," Nasjonal sikkerhetsmyndighet, 2020.

[6] "Nasjonal trusselvurdering 2021," *Politiets Sikkerhetstjeneste (PST),* 2021.

[7] "Nasjonalt digitalt risikobilde 2021," Nasjonal Sikkerhetsmyndighet (NSM), 2021.

[8] "Fokus 2021," Etterretningstjenesten, 2021.

[9] P. M. Salmon, G. J. M. Read, G. H. Walker, M. G. Lenné and N. A. Stanton, "Distributed Situation Awareness in Road Transport," 2018.

[10] "ISO/IEC 27001:2017". 2017.

[11] "ISO/IEC 27002:2017". 2017.

[12] "EKANS Ransomware and ICS Operations," *Dragos,* 2020.

12.1 Informative references

Datakvalitet ved digitalisering i petroleumssektoren (Data quality in digitalisation processes in the petroleum sector), SINTEF 2020.

Premisser for digitalisering og integrasjon IT – OT (Principles of digitalisation and IT-OT integration), SINTEF 2020.

Aktørenes tilstandsvurdering, vedlikehold og oppfølging av sikkerhetskritiske funksjoner og utstyr (How the players assess the condition of, maintain and follow up safety critical functions and equipment), SINTEF, 2018.

Datakvalitet ved digitalisering i petroleumssektoren (Data quality in digitalisation processes in the petroleum sector), SINTEF, 2020.

Digitalisering i petroleumsnæringen (Digitalisation in the petroleum industry), IRIS, 2018.

Cyber security in the oil and gas industry based on IEC 62443, DNVGL, 2018.

IKT-sikkerhet – Robusthet I petroleumssektoren – Regelverk og tilsynsmetodikk (ICT security – Robustness in the petroleum sector – Regulations and supervisory methodology), DNVGL, 2020.

ISO/IEC 27005:2018

ISO/IEC 31000:2018

IEC 62443

13 Appendix 1 - Relevant incidents

13.1 Triton/TRISIS 2017

Triton/TRISIS was a deliberate attack that occurred in 2017. The malware used in the attack was capable of making changes to safety instrumented systems (SIS). The Triton malware made it possible for the threat actor to adjust defined control levels in SIS. This meant that if, for example, there was excessive pressure in a gas turbine, it would not generate an alarm or trip signal. Knocking out the final safety mechanism can have enormous consequences, and entail a risk of prolonged production shutdowns, environmental emissions and danger to human life. The actions taken in the Triton attack show that, in reality, the threat actor must have had the objective of causing one or more of these consequences.

13.2 Ransomware virus

A new ransomware virus known as "Ekans" was detected in 2019. In addition to encrypting computer systems, Ekans had specific ICS functions for the purpose of, among other things, stopping ICS processes. According to the industrial cybersecurity company Dragos, this ransomware virus was unique and one of the first known ransomware viruses to have ICS-specific operations [1].

In May 2021, Colonial Pipeline, which is one of the USA's largest pipeline systems for transporting refined oil products, was also the target of a ransomware virus. The ransomware infected computer equipment that administered the pipeline, which forced operators to carry out a full shutdown.

13.3 Ransom-DDoS Attack at Telenor in 2020

In October 2020, Telenor reported that they had been hit by a rDDoS attack. The perpetrators launched a DDoS attack against Telenor, and then demanded ransom money to not expose Telenor to further attacks [2]. A ransom-DDoS (rDDoS) attack is a form of denial-of-service attack in which a threat actor threatens to carry out a DDoS attack against the target unless a ransom is paid to the threat actor.

13.4 The supply chain attack on SolarWinds in 2020

SolarWinds was the target of a supply chain attack in 2020. SolarWinds offers Orion, which is a network management system (NMS) that is used as a cybersecurity system. The attack occurred when a threat actor uploaded malware files onto SolarWinds' update server and included this in software updates. All customers who were diligent with their software update processes and updated to the latest version of Orion were infected with the malware, which included installation of a backdoor (known as "Sunburst") to the system. The threat actor thereby had access to all systems with this installation if it was exposed to the internet.

13.5 The supply chain attack on Kaseya in 2021

In July 2021, the software company Kaseya was also the target of a supply chain attack. This resulted in their customers receiving a software update that concealed a ransomware virus. Coop's cash register systems in Sweden were among those that received this update, and as a result, 800 stores had to remain closed for a week until the systems were back online.

13.6 The incident at the Mongstad Refinery in 2014

On 21 May 2014, the Mongstad Refinery experienced an unintended incident. The refinery had to switch to manual loading because an IT employee at the operations service provider HCL in India performed a restart of an incorrect server - a server that the operations service provider should not have had access to. The server that was restarted was one of Equinor's (then Statoil) production servers which controlled the automatic process for mixing and transferring petrol to tankers [3]. Equinor's employees who were physically present at the location had the expertise to take over the process, and were able to manually complete the process with minimal damage. In this instance, the consequence was a financial loss for Equinor of NOK 200,000-300,000. Large volumes of processes in oil and gas production are controlled by computer systems, and the consequence could therefore have been much greater depending on what had been affected. In 2017, it was announced that Equinor had brought the operation of safety-critical tasks from India back to Norway [4].

13.7 References for Appendix 1

[1] EKANS Ransomware and ICS Operations, Dragos, 2020.

[2] Telenor ble truset med pengekrav: Cyberkriminelle angriper og presser norske selskaper (Telenor threatened with ransom: Cybercriminals attack and pressure Norwegian companies), Telenor, 2020.

[3] Tastefeilen som stoppet Statoil, (The typing error that stopped Statoil), NRK, 2016.

[4] Statoil henter hjem sikkerhetskritiske IT-oppgaver fra India (Statoil brings home safety-critical IT tasks from India), NRK, 2017.