In proceedings of 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, 2016, pp. 510-516, https://doi.org/10.1109/ARES.2016.41

Cyber Security Incident Management in the Aviation Domain

Martin Gilje Jaatun
SINTEF ICT, Trondheim, Norway

Rainer Koelle
Lancaster University, United Kingdom

***Abstract*—Cyber Security Incident Management is an emerging paradigm and capability within the aviation domain. To date, limited research has addressed the requirements and developed tangible solutions for the deployment of such a capability. This paper leverages good practice and experiences from other critical infrastructure settings in order to sketch a recommendation for cyber incident response management for the aviation domain.**

***Keywords*-Incident Management; SWIM; SESAR; SJU; ATM Security; MSSC;**

I. Introduction

Cyber security is not a classical new problem in aviation, though originally the focus of aviation security was on the physical protection of aircraft and the prevention of 'bad persons' or 'bad items' boarding the aeroplane. Air transportation is experiencing a major transformation throughout the recent years with the introduction of state-of-the-art information systems in aircraft and ground systems.

The background and motivating need for a cyber security incident management concept in the aviation domain stems from the emergence of the System Wide Information Management (SWIM) service concept which is meant to improve information sharing in the future air traffic management (ATM) system [1]. SWIM moves from a tangle of point-to-point connections (Figure 1) to a coherent common one-to-many communication interface (Figure 2). The conceptualisation of SWIM as the 'aviation intranet' calls henceforth for a rethinking of security.

Whereas SWIM makes many aspects easier, it also increases the total complexity of the system; effectively creating a huge system-of-systems (SoS) which also introduces new security challenges. In particular, it must be noted that aviation is built on the principle of trust, meaning that a huge variety of stakeholders with very different interests operate jointly to ensure the safe and efficient transportation of passengers and goods. Accordingly, we face a SoS-context spanning these diverse stakeholders and their operational systems in a global context.

Recent research in the Single European Sky ATM Research (SESAR) programme revolved around motivating security measures for ATM assets by introducing a minimum set of security controls augmented by asset specific controls dependent on the criticality of the asset under investigation. Nonetheless, the interplay of security measures, the handling of in-situ security threats and attacks, and the joint procedures across such a SoS is still open. Other research attempts, e.g., the Global ATM Security Management (GAMMA) project, postulate a concept of operations that builds on national security operations centers recognising the need for a regional, i.e. European level coordination platform.

With the increased interconnection of ATM systems prompted by SWIM, the importance of having an efficient and effective scheme for handling cyber security incidents is highlighted. In this paper we will leverage good cyber security incident response practice [2], [3] and experiences from other critical infrastructure settings [4] in order to sketch a recommendation for incident response management for the aviation domain.

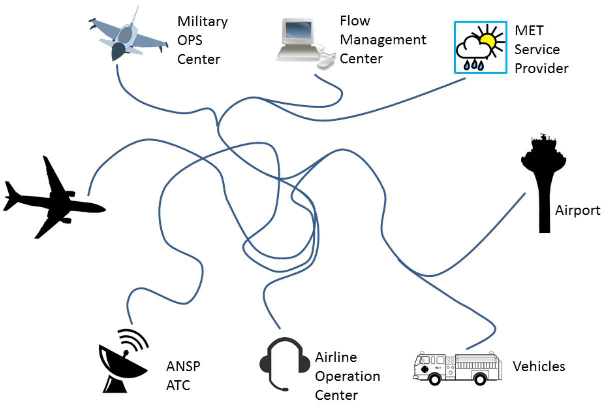

Figure 1: Aviation communication before SWIM [5]

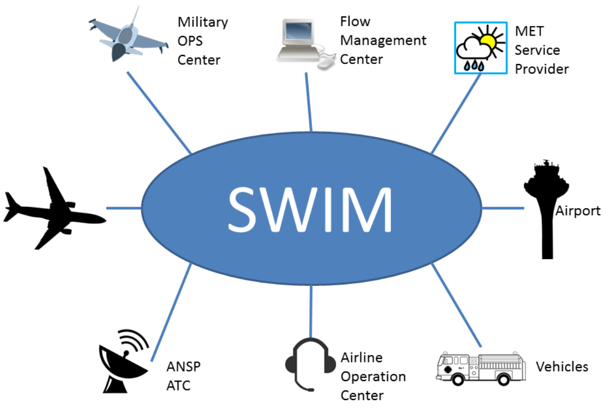

Figure 2: Aviation communication after SWIM [5]

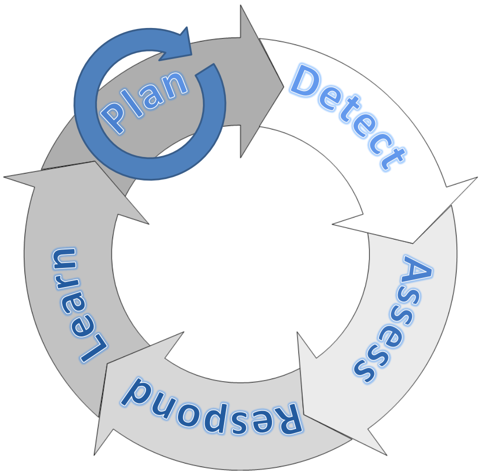

Figure 3: The complete incident management process (ISO/IEC 27035)

II. Incident Response Management

Information security incident management in an ATM network such as SWIM will by necessity be closely tied to the ATM domain, but there are important lessons to be learned from other critical information infrastructure domains, and SWIM information security incident management is thus initially based on such previous work [4].

Security incident management is an integrated part of the overall security management. It is important that security incident management is cleanly defined in the security policy, and that the objectives are stated. Thus, it is clear that information security incident management has a transversal scope. In some organizations there is a dedicated Computer Security Incident Response Team (CSIRT). In others, the security incident response teams are established ad hoc when an incident occurs. The organizational structure of security incident management should not be determined before the overall architecture of the SESAR ATM solution has been established and the security policy has been defined.

Throughout the recent years, the concept of security operation centers (SOC) has gained higher popularity in Europe. Some European Air Navigation Service Providers (ANSPs) has started to invest and established SOCs within their organisations, for example, ENAV in Italy and NATS in the United Kingdom. So far, the focus on SOC capabilities aims at establishing a central unit with the organisation charged with the identification of security incidents, their containment, and the forensics. As concerns the identification of security incidents, today's SOCs build primarily on pattern recognition and classical penetration testing or intrusion detection tools. The focus revolves around the protection of surveillance and flightplan data, and assocaited information processing systems and inter-organisational networks.

The proposed incident management cycle combines ISO/IEC 27035 [2] and NIST 800-61 [3] with increased emphasis on a reactive learning loop, focusing on improving governing variables such as organisational, human and technical factors, and proactive preparation. These reactive and proactive elements must be included in incident response management in order to ensure that incident response procedures are continually improved, and that lessons learned are disseminated to the appropriate parts of the organisation. Improving incident response will also improve the resilience of integrated operations and reduce the likelihood of severe incidents due to human errors as well as security incidents influencing safety of personnel, reliability and regularity of production.

The phases are interrelated. The Plan phase makes one ready to detect incidents in the best possible way, thus resuming to normal operation in the most efficient way. The Detect, Assess and Respond phases are triggered by an incident, but the actual detection and recovery work that is performed is based on preparations and proactive learning which have been performed in the Plan phase. The Learn phase follows automatically after the actual detection of incidents and the subsequent recovery from them. This learning is important as it makes it possible to improve activities in the Detection and Respond phases as well as in the Plan phase, and will provide useful input to the external dynamics that constitute the general security activities such as improvement of technical and organisational barriers. The Plan phase influences the learning phase as well by planning how reactive learning should happen.

The nature of SWIM will require the coordination of activities between different organisations. From that perspective the process depicted in Figure 3 will therefore have to take place on the SWIM level and within the different organisations. Only by interweaving the security processes of the different organisations (i.e., stakeholders), the anticipated goal of a secure SWIM SoS context can be realised.

A. Security Incident Management Plan Phase

The plan phase is where the organisation prepares to detect, handle and recover from attacks and other incidents. There is a need for documented incident management plans which are founded on a risk analysis. The risk level that is determined by the risk analysis and external information should be communicated to all relevant employees, and this should include information on unwanted incidents that have taken place in the past.

The information security incident management planning and preparation phase focuses on documenting the information security event and incident reporting and handling policy, and associated procedures; getting the appropriate incident management organizational structure and personnel in place; and instituting an awareness briefing and training program.

The incident management plan should consider organisational and human factors as well as technical issues, and must be designed to cope with the complex situation with operators and multiple contractors. The plan should focus on:

- Who is responsible for the different activities;

- When and how to perform the different activities.

It is important to realise that not all possible incidents can be described and appropriate procedures be defined. One fundamental capability is therefore to train operators and familiarise them with the overarching principles of the security policy. This ensures that decisions are made and aligned with these goals, even when unanticipated incidents unfold that require the application and refinement of plans and roles.

Our proposal for a SESAR Security Incident Management Cycle is basically the ISO/IEC 27035 cycle illustrated in Figure 3, with an additional focus on continuous learning and interaction with external dynamics. This means that the activities that are part of the Plan phase should be revisited, either periodically or because of incident learning, changes in risk, new working methods, etc., to ensure that preparations are continuously improved. The continuity of the Plan phase should be described in the plans with a focus on what triggers the different activities. The details of the Plan phase should be closely linked to the security policies of the organisation.

Plans and roles should be based on a risk-based approach. Plans and defined roles must be implemented and followed up by awareness-creating activities at individual and organisational level as well as training activities. Monitoring procedures and key performance indicators are also important inputs to decisions regarding how incident response plans and roles are designed. All the activities in the plan phase must furthermore be adjusted to external dynamics, e.g. changes in competency, or changes in the overall risk picture.

Incident response management does not operate isolated from other parts of the organisations and the organisational context. Incident response management is of course influenced by the general information security management strategy of an organisation. At the same time, information security management is influenced by incident response management, as information security management approaches must be adjusted to learning made in incident response management processes. Both information security management and incident response management are influenced by information security regulations.

In addition to information security management approaches, incident response management must operate together with other organisational processes and structures. Furthermore, the incident handling process must interact with changes in the global threat picture, technological change and innovation, and increased available information. This is a two-way street, in that the handling of incidents facilitates learning that is important to the general information security work in an organization. The information flow routines must therefore also ensure that system administrators and other relevant personnel become party to information (e.g., regarding new attacks and misconfigured equipment) from the learn phase.

Technical mechanisms such as Intrusion Detection Systems, firewalls and anti-virus software are vitally important in any modern computer network, and can detect (and often prevent) a large number of incidents in an automatic fashion. These mechanisms in themselves are outside the scope of SWIM Security Incident Management, but it is important that alerts and warnings that they generate are handled in the appropriate manner, and followed up by the incident response team. The main task in the Plan phase is thus ensuring that there are routines that facilitate the information flow, taking both organisational/human and technical aspects into account.

It is important to assess the probabilities and consequences of potential incidents that may occur, in order to prioritise activities and to identify if the mitigation represented by incident handling procedures is sufficient for a given incident type. Risk assessment of the relevant information systems should be performed regularly. To ensure that all relevant risks are identified, it is important to involve resources from ICT, process owners and supplier/contractor. The usual activities in such a risk assessment are:

- Organisation and planning of the risk analysis;
- Description of scope - defining object and relations to be analyzed;
- Identifying possible unwanted incidents (and if relevant – frequencies and consequences);
- Description of risks and assessment of risk;
- Identify actions to reduce probabilities and reduce consequences of incidents including contingency plans;
- Perform periodic assessment of the plan, and analyse relevant incidents to identify when the risk assessment should be updated.

This risk assessment should be an integral part of the overall security risk assessment for the information system, with the same assets. In addition, the possibilities for performing Real Time Risk Assessments on different parts of the Information System in the Respond phase should be investigated. In case of an incident, and given the time constraints for recovery in the ATM system, Real Time Risk Assessments would provide very important decision support to ensure that the right actions to mitigate the consequences of the incident are selected.

For some incidents, the competence of the suppliers of the equipment affected will be necessary to deal with the incident. At least for important systems, suppliers' responsibilities in case of incidents involving their systems should be included in contracts.

The responsibilities of contracted personnel and suppliers in case they detect or suspect an incident should be clearly stated and communicated. The responsibility for raising incident alerts should not only apply to internal employees, but everybody involved.

B. Security Incident Management Detect Phase

When incidents occur it is important to be prepared and have a plan for how to detect and handle the incident. It is recommended to create a plan for incident response, which consists of three main parts:

1) A plan on what to do when detecting or suspecting that an incident has occurred: this plan is directed towards all employees, including contractors and suppliers. It should be readily available (e.g. intranet, posters) and easy to understand, meaning that it should be short, precise and follow common terminology and common perceptions.
2) A plan for how to detect incidents with the help of tools, routines and information sharing: this plan is directed towards those responsible for the work on security.
3) A detailed plan for how to respond to different types of incidents: this plan is directed towards those responsible for recovery from incidents.

A critical aspect of the detection phase is the identification of the incident and the appropriate level of response. This includes the launch of procedures (e.g. alerting staff/colleagues, informing managers or relevant authorities) as well as the initiation of rehearsed or prepared actions (e.g., disabling of processing nodes). While the latter is refined in the next phase, it is inherent to recognise that early response is closely linked with successful detection.

C. Security Incident Management Assess Phase

When the incident alert reaches someone that is responsible for handling the incident, the incident should be assessed to determine the severity of the incident and the way forward.

Conceptually, the assess phase is targeted at positively identifying an incident. As mentioned above, the detection phase delivers the evidence on which now – during the assess phase – an appropriate evaluation needs to be made. In principle, the assess phase aims at

- determining whether the event is an actual security incident or a false alert
- categorising the identified incident – for example – as minor or major
- triggering the respective response procedures given the categorisation

The assess phase can be broadly described as an incident confirmation and plan selection process. From that perspective, the assess phase is a critical milestone in the timely and targeted response to an incident. Given the assessment, resources and procedures are initiated that themselves might require resources. It is therefore important to provide clear guidelines and decision patterns for this phase. The incorrect assessment or initiation of a wrong plan can ultimately require lengthy correction measures.

D. Security Incident Management Respond Phase

In order to recover successfully and effectively from an incident, it is important to be well prepared, meaning that a plan and the necessary skills are in place. This is where careful work in the Plan phase will pay off. Important factors are:

- Clear responsibilities – distributing the responsibility for incident management activities through an appropriate hierarchy of personnel, with assessment decision making and actions involving both security and non-security personnel';
- Clear procedures – providing formal procedures for each notified person to follow, including reviewing and amending the report made, assessing the damage, and notifying the relevant personnel (with the individual actions depending on the type and severity of the incident)'.

When an incident is under control it should be identified what further responses are required to bring the system back to normal operation. This is the time for restoring systems, assuring that systems are in a safe condition, reconnecting to external networks, etc. In this process it will often be necessary to:

- Take immediate actions to reduce the vulnerability of the system: install necessary patches or improve the configuration of the system by changing passwords or disabling unused services.
- Utilize tools: installation media, backups and recovery tools, and possibly also integrity checks and investigation tools.
- Be aware of malicious code: trojans, rootkits and kernel modules can be maliciously placed in the current system, and are hard to detect.

Often it is considered that losing some data is better than a (still) insecure system. In an ATM setting it is however important to balance the need for improved security and the need to keep the system up and running. To put it bluntly, you cannot reboot a plane in the air. It is therefore important that representatives from both IT and the ATM actors (air traffic controllers, etc.) are involved in decisions that will result in a shutdown of the system, or that may render the system unstable.

When everything is up and running and the incident handled it is important to use the experiences made as an opportunity for improvement. The documentation created during incident detection and recovery, and the experiences made by those involved in handling the incident can be used to improve the preparedness of the organisation to prevent and handle incidents in the future. This is the focus of the Learn phase. The activities of the Learn phase should be started when the incident is still fresh in peoples mind. But first: Remember to provide status information to the individual that raised an alert about the incident. This is an important part of the work on awareness when it comes to incident management.

E. Security Incident Management Learn Phase

This phase covers the learning process that follows an incident that has happened. Proactive learning related to anticipation – knowing what to expect – are treated in the Plan phase.

Incidents should be used as an opportunity for learning and improvement. Learning from incidents should be a planned part of incident handling, and the necessary resources must be allocated. The learning process is focused on organisational learning. The aim is to change the incident response based on the difference between expected and obtained outcome (single loop learning) in addition to be able to question and change governing variables related to technology, organisation and human factors that lead to the outcome (double-loop learning).

The focus is on what led to the incident, what happened, and how the incident was handled, by understanding how the incident happened and analysing barriers; and by understanding how the incident was handled and analysing improvements by using a post-mortem analysis.

In order to be able to succeed with organisational learning, the organisation must be prepared for learning. The management must decide on the resources to be used. The key issue is the extent of management commitment to learning and the willingness to use resources in learning from this type of incidents. For each incident, a consideration should be made regarding to what extent one is able and willing to learn from this incident. This is highly related to the seriousness of the incident, and will decide the amount of resources that will be used on learning from the incident.

III. Logging, Reporting and Monitoring

A. Logging

As part of the overall SWIM Security there should be established logging and monitoring in real time at key points in the information system. The use of the logging and monitoring data in SWIM Security Incident Management would be

- To detect irregularities in the information system that could lead to incidents;
- To aid in the detection of incidents in the Detect phase;
- To support forensics in the Respond and Learn phases.

B. Reporting

A system for reporting the handling of Incidents should be established. The reporting should identify what happened, including:

- The causes of the incident;
- What it resulted in, i.e., how the Information System was affected;
- How it was handled, step by step;
- The consequences of the incident and what was done to mitigate the consequences.

C. Monitoring

The performance of the SWIM Security Incident Management should be monitored to ensure the efficiency of handling the incidents and learning from incidents. To support the monitoring a set of key performance indicators should be identified, such as:

- Rating system for the incident response management system;
- Assessment of information security culture regarding incident response;
- Number of incidents responded to;
- Average time spent on responding pr incidents;
- Total consequences of incidents;
- Number of incidents of high loss;
- Downtime of ATM systems;
- Total costs related to incident response.

D. Security Incident Management Requirements

Some of the requirements for security incident management are already covered by requirements identified for ATM self-protection [5]. Additional requirements are identified in D03 [6]:

- The SWIM Infrastructure shall establish logging and monitoring in real time at key points in the information system. The use of the logging and monitoring data in SWIM Security Incident Management shall detect irregularities in the information system that could lead to incidents; aid in the detection of incidents in the Detection and Reaction phase, support forensics in the Recovery and Learning phases.
- The SWIM Infrastructure shall establish a system for reporting the handling of Incident. The reporting shall identify what happened, including: the causes of the incident; what it resulted in, i.e. how the Information System was affected; how it was handled, step by step; the consequences of the incident and what was done to mitigate the consequences.
- The performance of the SWIM Security Management shall be monitored to ensure the efficiency of handling the incidents and learning from incidents. To support this monitoring, a set of key performance indicators shall be identified, such as: rating system for the incident response management system; assessment of information security culture regarding incident response; number of incidents responded to; average time spent on responding pr incidents; total consequences of incidents; number of incidents of high loss; downtime of systems; and total costs related to incident response.
- Data processing of ATM information exchanged through the SWIM shall allow for it to be made available to authorised security organisations.

IV. An Aviation CERT for Europe?

The major requirement in moving towards a joint cyber security incident management capability in aviation is the establishment of a cyber security policy. At the time being, attempts to develop such a policy are fragmented and left to regional or national activities. Aviation is a global business and as such requires a global policy to be implemented worldwide. This puts the International Civil Aviation Organization (ICAO) in the spotlight of attention. While ICAO is currently pursuing a tremendous harmonisation effort in terms of aligning the regional attempts to facilitate the transformation to the new aviation environment (e.g. Europe: SESAR, United States:

NextGen, Asia-Pacific: CARATS), the focus is on harmonising operational concepts and enablers. The aspect of security is widely not postulated. One of the key impediments is the fact that the ICAO Aviation Security Panel is only slowly recognising cyber security as its task on top of the classical physical oriented aviation security dimensions.

In the absence of a clear global policy, it can be seen that regions like Europe and the US struggle in implementing their security posture. Different aspects have led to this situation. For example, the sequestration in the US or the reprioritisation in Europe led to the fact that security achievements in SESAR and NextGen are outsourced to the development phases. The latter can also be derived from the reiteration of high-level 'cyber security requirements' in the most recent SESAR deployment plan.

The SESAR development phase developed the concept of so-called minimum set of security controls (MSSCs). This set of controls offers a base level of security that can be compared to other critical infrastructures. Nonetheless, this base level needs to be augmented with security controls for systems related to the core functions of ATM: the separation and synchronisation of air traffic. The latter will see the majority of surveillance and communication systems and networks becoming critical assets. Security measures for these systems need to be aligned and supported by a CERT capability across Europe and the wider global context.

Based on this global perspective, incident response plans and measures can be devised that address the cyber incident information exchange and crisis coordination, including the establishment of timely escalation mechanism from local to regional or global level. The latter suggests that associated coordination centers are required on regional and global level to establish the fundamental instrument for coordination, information sharing, lessons learned, and adaptation of response plans.

Based on the discussion in this paper, the basic four capabilities can be identified for an aviation CERT:

- **Establishing a CERT capability:** on a global scale such a capability has to be postulated as part of the ICAO aviation security policy, including the requirement for establishing regional and national coordination centers. It must be recognised that aviation cyber security incident handling cannot be limited by national sovereignty issues and that appropriate authorities shall be given to these aviation CERT centers. These centers need to be appropriately staffed and financed.
- **Establishing an operational capability around the incident cycles:** the portfolio of activities need to span the incident cycle phases discussed in this paper. This includes the proactive information sharing and learning as well as the identification of appropriated preparedness action. Appropriate detection and assessment capabilities will require a higher integration of the security capability within the SWIM context. While SWIM can serve as the platform for security management, it also needs to support appropriate technological means. Hence, the current suite of information exchange models need to be augmented with dedicated security incident information exchange models and artifacts that support the operational capability [7].
- **24/7 operations:** while the aforementioned points establish the framework and the infrastructure for an aviation CERT, the 24/7 operating mode needs to be ensured through appropriate resources. With a view to the diverse stakeholder base this poses challenges. However, integrative models of operations allow for a wide participation from different stakeholders.
- **Cooperation:** as cyberspace is borderless and aviation is a global industry, collaboration is a key requirement for the aviation CERT capability. Emerging threats, identified vulnerabilities, and observed incidents in cyberspace in other sectors and industries offer insights in potential incidents and allow for a tailoring of aviation related response plans. Accordingly, other industries can benefit from lessons learned in aviation.

V. Conclusion

We have presented a scheme for cyber incident response management in the aviation domain, based on existing standards and good practice from other critical infrastructure domains.

There are relatively few empirical studies of cyber security incident response management [8], and also in this case we expect that the proof of the pudding will be in the eating; i.e., only after implementation of this scheme in an ecosystem that includes an aviation CERT will we see the full implications.

Acknowledgements

This paper draws heavily on previous work performed in the IRMA project [9], with contributions from Eirik Albrechtsen, Maria Bartnes, Stig Ole Johnsen, Odd Helge Longva, Inger Anne Tøndel and Irene Wærø. This paper also contains results of collaborative research co-funded by the SESAR Joint Undertaking. However, the paper does not purport to represent the views of SESAR JU or any SESAR partner.

References

[1] M. Krempel and M. G. Jaatun, "Learn to SWIM," in *Proceedings of ARES 2014*, 2014, pp. 556–560.

[2] "ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management," 2011.

[3] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "NIST SP 800-61: Computer Security Incident Handling Guide," National Institute of Standards and Technology, 2008.

[4] M. G. Jaatun, E. Albrechtsen, M. B. Line, I. A. Tøndel, and O. H. Longva, "A framework for incident response management in the petroleum industry," *International Journal of Critical Infrastructure Protection*, vol. 2, pp. 26–37, 2009.

[5] M. G. Jaatun and T. E. Fægri, "Sink or SWIM: Information Security Requirements in the Sky," in *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, Sept 2013, pp. 794–801.

[6] M. Brochard, N. Bleifuss, T. Ozdemir, M. Kutilek, M. D. Cat, J. Stevens, M. G. Jaatun, O. H. Longva, A. Giordano, S. Herve, and A. Berna, "SWIM Security Context and Needs Analysis," SESAR Project 14.02.02 SWIM Security Solutions Deliveravble D03.

[7] C. Frøystad, E. A. Gjære, I. A. Tøndel, and M. G. Jaatun, "Security incident information exchange for cloud services," in *Proceedings of International Conference on Internet of Things and Big Data*, 2016.

[8] I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature," *Computers & Security*, vol. 45, no. 0, pp. 42 – 57, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404814000819

[9] M. G. Jaatun, S. O. Johnsen, M. B. Line, O. H. Longva, I. A. Tøndel, E. Albrechtsen, and I. Wærø, "Incident response management in the oil and gas industry," Tech. Rep., 2007, SINTEF Report A4086.