

**FINAL REPORT**

**ENCO-FR-(19)-12 / May 2019**

**HOME/2015/ISFP/AG/CBRN/3000008463**

Mitigating the Insider Threat at Chemical Facilities with Precursors to Explosives

****

Project funded by the European Union

|  |  |  |
| --- | --- | --- |
|  |  |  |

DOCUMENT REVIEW AND APPROVAL COVER SHEET

|  |  |
| --- | --- |
| **PROJECT Nr.:** | HOME/2015/ISFP/AG/CBRN/3000008463 |
| **PROJECT TITLE:** | Mitigating the Insider Threat at Chemical Facilities with Precursors to Explosives |
| **PERFORMED BY:** | ENCO and SCK•CEN |
| **DELIVERABLE:** | Final Report |
| **PREPARED FOR:** | European Commission |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DATE released | REVISION | PREPARED/REVISED by: | REVIEWED by: | APPROVED by: |
|  |  |  |  |  |
|  |  | Ahmed Nagy SCK•CENMichiel Van Oudheusden SCK•CENChristine Tomic ENCO | Christine TomicENCO |  |

**Disclaimer**: The content of this report does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

**Acknowledgments**: This research project was funded by the European Commission Internal Security Fund through the “implementation of the CBRN Action Plan, the EU Action Plan on enhancing the security of explosives and the European programme of critical infrastructure protection”. The research team would like to thank all the participants who made it possible to carry out data collection and research visits.

Table of Contents

[Executive Summary 4](#_Toc8904085)

[Methodology 5](#_Toc8904086)

[1 Introduction 6](#_Toc8904087)

[2 Motivation 7](#_Toc8904088)

[3 Objectives 9](#_Toc8904089)

[4 Problem definition and scope 9](#_Toc8904090)

[5 Concepts and Definitions 10](#_Toc8904091)

[6 Interaction with industry 12](#_Toc8904092)

[6.1 Analyzing Insider Threat through a Crime Theory lens 12](#_Toc8904093)

[6.1.1 Increase effort 12](#_Toc8904094)

[6.1.2 Increase Risk Perception 14](#_Toc8904095)

[6.1.3 Reduce Rewards 14](#_Toc8904096)

[6.1.4 Reduce Provocation 15](#_Toc8904097)

[6.1.5 Reporting 15](#_Toc8904098)

[6.1.6 Remove Excuses 15](#_Toc8904099)

[6.1.7 Social Responsibility 16](#_Toc8904100)

[6.2 Relevant Attributes and Dimensions of Insider Threat Analysis 16](#_Toc8904101)

[6.2.1 Trust 17](#_Toc8904102)

[6.2.2 Organizational Culture 18](#_Toc8904103)

[6.2.3 Security Culture 18](#_Toc8904104)

[6.2.4 Safety culture 19](#_Toc8904105)

[6.2.5 Data culture 20](#_Toc8904106)

[7 Barrier Selection and Adoption 21](#_Toc8904107)

[8 Limitations 22](#_Toc8904108)

[9 Recommendations 23](#_Toc8904109)

[10 Resources 25](#_Toc8904110)

[11 Conclusion 26](#_Toc8904111)

[12 References 27](#_Toc8904112)

Table of Figures

[Figure 1 Effectiveness of policing strategies adapted from [Clarke 2005] 15](#_Toc8903252)

[Figure 2 A summary of the main trust attributes in an organizational context 18](#_Toc8903253)

[Figure 3 Relevant barrier Selection Factors 22](#_Toc8903254)

# Executive Summary

Minimizing the Insider Threat in the supply chain of precursors to explosives was a two year (February 2017-May 2019) long research project, funded by the European Commission through the CBRN Action Plan specifically the Action Plan on enhancing security to explosives and the European program for critical infrastructure protection. The project was motivated by a shared concern from stakeholders (policy makers, regulators, industry representatives and employees) that certain groups (i.e. insiders) would still have access to precursors to explosives, in possibly even larger quantities than the general public despite Regulation No. 98/2013 being enforced throughout the EU MS. The common conviction was that Annex 1 and 2 of Regulation No. 98/2013 limits the use of identified chemical precursors to explosives to the general public and registered professional users, but not to employees and individuals from the supply chain. This project has been devised in order to close the gap, conceptually, thereby increasing public security within the EU in full compliance with the fundamental rights of its citizens. Due to the widespread global use of some of the chemicals listed in Annex 1 and 2 of Regulation No. 98/2013, regulating their appropriate usages from both the general public’s as well as industry perspective should be at the core of industry values. Hence, industries have a responsibility to guard against potential security threats emanating from “insiders” with malevolent intentions, including individual’s intent on committing acts of sabotage or theft. To identify relevant insider threats and sensitize stakeholders to them, the project explored four major sub categories in the supply chain: the production, transportation, storage and professional users for three chemical precursors (Nitric Acid, Hydrogen Peroxide, Ammonium Nitrate); each of which constitutes a potential security threat in terms of explosive precursors (TNT, TATP, ANFO). The project builds on the already existing regulation on the Marketing and Use of Explosive Precursors Regulation No. 98/2013 by utilizing its fundamental framework (the Annexes) and extending it to cover the whole supply chain (i.e. insiders). As an attachment to this report, the final result comprises of a Handbook of Smart Measures to serve as holistic interactive mechanism for industry to use to help mitigate against insider threats in the chemical industry.

# Methodology

The project drew on a range of explorative research methods and fieldwork, resulting in a Handbook containing insider attack scenarios for each chemical and subcategory, as well as a set of barriers (smart measures to specifically dispel said scenarios), guides on insider attributes and characteristics, mechanisms to conduct spot checks on the security status and safety and security culture as well as recommendations for implementing improvement actions, behavioral attributes for management and personnel in institutions and how those may work to minimize insider type behaviors as well as guiding questions to consider when building a security regime and several high level recommendations tailored to mitigating the insider threat. The methodology included both quantitative and qualitative approaches that relied on first-hand observations, semi-structured interviews, researchers’ expertise and experiences, subject matter experts, document analysis and “walkthroughs,” and guided tours of the critical industry infrastructures with research participants. Some organizations were visited multiple times and some interviewees were consulted several times. During the project, research investigators met at repeated intervals to discuss tentative findings and further scope their research approach. The project was presented and discussed at various industry association meetings, in order to raise awareness on the project and the insider threat concepts. Further, the research team used multiple forums to gain insight and input from a wider industry audience. The project teams engaged with policy and decision makers, regulators, industry managers, and employees. They used their own expertise acquired from relevant disciplines in order to develop strategies to identify, and remedy the insider threat, learning from comparable strategic industries. The methodology applied built on proven approaches to mitigate the insider threat in the nuclear, aviation, pharmaceutical, food processing and IT industry, combined with concepts of industry general security practices. The approach followed is based on the development of scenarios that takes into account all parameters of relevance (selected 3 precursors chemicals and 4 product life cycle subcategories), from the minimal qualities needed to make an explosives device to the accessibility of the precursor. The development of scenarios established an ideal basis for the identification of measures that would prevent a scenario from being completed. The measures themselves are a combination of prevention techniques in the misuse of assets developed in the nuclear, aviation, pharmaceutical, food processing and IT industry, as well as newly developed barriers which directly reflect the specific needs within the chemical industry. The barriers and scenarios have been tried and tested through interaction with industry. They were further grouped, indicating which structures need to be in place for the measure/ barrier to be effective; for more details please consult the Handbook.

Furthermore, during the strenuous research conducted the project team built on attributes and characteristics of the insider, how a potential insider can be recognized, and what the motivations might be. These are to help industry understand the insider concept, but also to be able to include such characteristics in their security mechanisms. Furthermore, safety and security culture examples have been drawn up from critical strategic industries in order to further aid the chemical industry in making sure its culture and structures are robust enough to withstand and mitigate against a possible insider. These and additional mechanisms for spot checks, management and personnel behaviors to describe insider type behaviors and more are included in the Handbook.

# Introduction

European nations are confronted with new and complex security threats, both physical and virtual. As the European Commission highlights in its 2015 European Agenda on Security, many of these threats originate from instability in the EU’s immediate neighborhood and changing forms of radicalization, violence, and terrorism. Not only are threats becoming more varied and dispersed, they are increasingly cross-sectorial in nature, affecting different industry sectors. It is therefore of utmost importance, in the coming years, to raise security awareness, amend laws, centralize and exchange data and deliver guidelines to the population and specific strategic industries in order to decrease and manage the threats challenging our daily way of life. Critical industry sectors are at the forefront of this paradigm shift and need to be leading the way in order to ensure the security of our populations in these changing security climates.

Although critical and sensitive industries have reasonably well-developed strategies for protecting against external threats, sabotage, and intrusion, the situation changes dramatically when sabotage or theft is perpetrated or supported by insiders. It can therefore be argued that the insider threat is the biggest residual remaining threat to strategic industries. Unlike conventional threats, where increasing physical security measures, controlling access and similar measures help minimize risk, to combat insider threats a range of complementary measures need to be in place. This is in particular relevant for access to precursor material, dangerous substances and other dual use items and materials. While restrictions might limit the general public gaining access to (certain quantities) of substances, materials and goods, unrestricted access to practically unlimited quantities is available to staff of a facility – insiders.

The damage that could be caused by insiders with malevolent intentions and the ease of access insiders have to precursors to explosives and dangerous materials makes this topic highly relevant. Other critical industries, such as the nuclear, aviation, pharmaceutical, food processing and information technology industry, have been successful in controlling substances, information, and access without undermining legitimate activities. This project poses the opportunity for the chemical industry to do the same by utilizing the tools developed.

# Motivation

Explosives precursors are chemical substances that can be (and have been) misused to manufacture explosives (homemade and others). Regulation No. 98/2013 on the marketing and use of explosives precursors, applicable since September 2014, has two core objectives: 1) to increase public security through a reduced risk of misuse of explosives precursors for the manufacture of homemade explosives; 2) to enable the free movement of explosives precursor substances in the EU internal market, given their many legitimate uses. The regulation forms a system of restrictions and control mechanisms on a number of explosives precursors with the aim of limiting the general public's access to these substances. The regulation also establishes an obligation for operators to report suspicious transactions, disappearances and thefts of explosives precursors.

A report authored by the European Commission in consultation with the stakeholders confirmed the existence of significant challenges related to the application of the regulation, including insufficient awareness along the supply chain on the rules and obligations arising from the regulation. Further, the present regulation does not refer to threats arising from insiders or mechanisms to manage such threats. For instance, Article 9 of Regulation No. 98/2013 states that economic operators are obliged to report “significant” disappearances without specifying what this means and without mentioning insiders:

“Economic operators shall also report significant disappearances and thefts of the substances listed in the Annexes and of mixtures or substances containing them to the national contact point of the Member State where the disappearance or theft has taken place.”

Thus, while the present Directive effectively focuses on external risks, it does not provide guidelines or identify risks that might originate from insider activities.

To address this lacuna, three substances were chosen from the two annexes of materials attached to Regulation 98/2013, which are described as follows:

1. Substances which shall not be made available to members of the general public on their own, or in mixtures or substances including them, except if the concentration is equal to or lower than the limit values set out below.
2. Substances on their own or in mixtures or in substances for which suspicious transactions shall be reported.

Two of the substances are from Annex 1 while the third is from Annex 2. A quick review of the explosion events[[1]](#footnote-1), [[2]](#footnote-2) in the last 30 years (starting from 1988) that used chemical substances shows that Nitric Acid, Ammonium Nitrate are among the top ten substances used while Hydrogen Peroxide comes as an attractive substance for malicious actors targeting areas with high security surveillance due to the absence of nitrous compounds and the difficulty in detection. The substances chosen are both solid and liquid which was reflected in the design of the scenarios and barriers for the Handbook.

|  |  |  |
| --- | --- | --- |
| **Nitric Acid (Liquid)** | Annex 1 | Relevant to TNT |
| **Ammonium Nitrate (Solid)** | Annex 2 | Relevant to ANFO |
| **Hydrogen Peroxide 70% above (Liquid)** | Annex 1 | Relevant to TATP |

As a result, the substances chosen are representative to the different challenges and risks they pose in handling and theft during the different supply chain phases. Further, the substances were chosen to span the needs of the relevant industries. The table below provides a concise overview of the three substances identified to carry out the study.

The three chosen chemicals are precursors to explosives. It was determined that Nitric Acid to explosive material 0.8:1 which is used for TNT, Hydrogen Peroxide to explosive material 1:2 which is used to make TATP (the mother of Satin) and Ammonium Nitrate to explosive material 0.95:1 which is a precursor to ANFO. Home Made Explosives (TATP and ANFO fall under this category) have been the most common type of explosive used in recent terrorist IED attacks in Europe and beyond. To date, the explosive used in a wide variety of attacks is Triacetone Triperoxide (TATP), a home-made explosive that remains the explosive of choice for terrorists, due to its rather simple composition. The internet continues to be a crucial resource for lone actor terrorists to gain bomb-making skills. Internet websites, forums, social networks and the Darknet facilitate access to bomb-making knowledge and information. Furthermore, the chemicals range from liquid format to solid; thus, the attack scenarios and barriers for mitigation namely the smart measures could be transposed to other chemicals in the same format (i.e. liquid chemicals some nitric acid and hydrogen peroxide scenarios could be used and solid from the ammonium nitrate).

It should be noted that although thus far no explicit link has been established between insider theft and terrorism, it would be imprudent and irresponsible not to explore this connection and anticipate risks associated with it – especially as even low amounts in the order of a few hundred grams can cause significant damage to humans or facilities.)[[3]](#footnote-3) Furthermore, a suicide vest typically weighs between 15-20kg, given the above ratios it becomes clear that an insider (who has access to precursor material, and time) would have little difficultly to access the quantities of material necessary to build several suicide vests posing a significant threat to the populations but also structures.

For the same reason, the project explicitly focuses on the full life cycle of the three abovementioned precursor chemicals, from production to transport, storage, and professional end use. It is assumed that by focusing on the whole life cycle of the precursor chemical, measures to mitigate insider threats are likely to be more effective.

# Objectives

This study aimed at exploring relevant concepts and definitions to ‘insider threat’ within the context of the chemical industry and precursor explosive substances. For this purpose, the project team analyzed applicable literature and carried out field studies and visits to relevant facilities and bodies in the chemical industry in Europe. The project’s objectives are listed below.

**Objective 1:** To explore key terms and concepts related to insider threats in fields that can benefit the chemical industry.

**Objective 2:** To identify effective approaches for risk mitigation of insider threat in the chemical industry with a main focus on theft.

**Objective 3:** To provide the industry with an effective approach and tools to improve risk awareness and mitigation for insider threats (Deliverable: Handbook of countermeasures).

# Problem definition and scope

Insiders have three crucial attributes which can potentially maximize damage to a facility: 1) knowledge, 2) time, and 3) access. The insider threat is becoming a dominant residual risk in critical industries [Baracaldo 2013, Baracaldo & Joshi 2015], as such it is imperative to carefully monitor potential insider security breaches and mitigate possible risks.

According to [Baracaldo 2013] the insider threat risks are characterized by the following features:

* Insider threats can be hard to detect.
* It is tough to differentiate harmful actions from regular work.
* It is relatively easy for employees/insiders to cover their actions.
* It is can be hard to prove malevolence of insiders.

For these reasons, specific measures are necessary to mitigate the insider threat – measures that do not interfere with work cycles and productivity whilst at the same time do not cause a coercive environment within the facility. While restrictions or regulations might limit the general public from gaining access to certain quantities of substances, materials and goods, unrestricted access to practically unlimited quantities is available to facility staff. Although different industries and businesses opt for monitoring solutions such as surveillance, surveillance approaches and barriers have their limitations towards insider threat mitigation. A holistic approach needs to be developed to face the challenges and risks that come with insider threats. While it is impossible to completely eliminate the insider threat, a solid insider threat mitigation programme can greatly reduce the prevalence of associated risks and the impact on organizations being attacked ‘from within’.

# Concepts and Definitions

The current section presents some of the main definitions relevant to the project scope. The focus is maintained on the European context since the work planned was expected to address the limitations of addressing insider threat for European chemical facilities. The definitions used are *living* - definitions that were/ are continuously revisited during the lifetime of the project and beyond. The initial set of definitions has been identified based on the nuclear industry and the information technology industry which have been identified as two industries that can benefit from a more systematic study of the insider threat [IAEA 2008] and [Cole 2005]. Whereas every concept has a core or minimal definition, which is accepted by most users, this minimal definition can be expanded to allow for the development of more specific meanings, suited to a particular setting or context. For instance, while barriers are meant to enhance security, the notion of barrier takes on different forms in different organizations and settings. Barriers may be natural, technological, behavioral, or organizational.

Below is a list of the main relevant working definitions.

* **Insider:** An individual with authorized access to chemical facilities or material in transport who could attempt unauthorized removal or sabotage, or who could aid another internal or external adversary to do so.[[4]](#footnote-4)
* **Adversary:** The term is used to describe any individual performing or attempting to perform a malicious act. (IAEA identification of vital areas at nuclear facilities guide).
* **Normal operation:** Is composed of activities that help support or result in the production of the products synthesized in the different target factories or facilities to meet client demands and stakeholders announced legal interests (this also extends to transport and storage).
* **Threats:** Potential events or actions that can result in deviation, disruption or interruption of “normal operation”.
* **Insider threat:** Sabotage or theft that might be committed by “insiders”. Theft is the main focus of the current project due to its relevance for HME.
* **Evidence:** Precursors of events that can be correlated with the occurrence of threats and exploitation of vulnerabilities.
* **Barriers:** Actions, measures, methods that can decrease the probability of occurrence of malicious event (theft) or help log the different accompanying events taking place before the threat/s.
* **Facility:** A place, amenity, or piece of equipment provided for a particular purpose (i.e. includes all modes of transportation the facility automatically becomes a truck, a ship etc.)
* **Chain of custody:** The chronological documentation or trail, showing the possession, control and transfer, of physical or electronic material or evidence.
* **Risk:** the likelihood of a hazardous situation and having to deal with its consequences if it occurs.
* **Trust:** the belief that others at worst, will not, knowingly or willingly do you harm, and will, at best, act in your interests (or in this case the interests of the organization). [Newton 2018]
* **Organizational culture:** the importance of symbolism of rituals, myths, stories legends, interpretation of events, ideas, experiences that are shaped and influenced by the groups within the organization and a system of common symbols and meanings that provides the shared rules governing cognitive and affective aspects of membership in an organization. [Frost et al. 1985 & Kunda 1992]. Culture is a core ingredient in comprehending rules, behaviors, events institutions and process [Heijes 2011]. The interpretations of rules and actions is interpreted given the rule of meanings that lead different behaviors and consequences of the rule. Culture can be viewed as perspective not as solid artifact; thus, an auxiliary context where actions and rules are interpreted [Hatch 1993].
* **Safety culture**: is defined by IAEA as the assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, plant safety issues receive the attention warranted by their significance (p. 1) [IAEA 75-INSAG-4].
* **Security culture**: security culture is defined by the United Kingdom Center for Protection of National Infrastructures as the set of values, shared by everyone in an organization, that determine how people are expected to think about and approach security[[5]](#footnote-5).

|  |
| --- |
| **Synthesized Definition of an Insider based on the Project Team’s Field Work:**Throughout the project an insider was considered to be a human being who is deliberately acting in a way that puts the organization or the facility he / she is connected to at risk.  |

It is unfeasible to assume that an insider threat risk can be completely eliminated. However, it is realistic to work on risk regulation and minimize the probability of an insider threat situation from occurring. The residual risk is defined here as the risk after applying different control barriers and mechanisms to reduce risk to the business to a non-disruptive level. Celikel [Celikel et al 2009] presented an approach for risk calculation; which can be calculated by using the expected value formula multiplied by the impact cost of an event. A similar approach can be applied to an assessment of insider threat in conjunction with applying the proper suitable barriers. As long as the residual risk is in an “acceptable range”, the different activities can be carried at a reduced risk after the application of proper barriers, countermeasures and update of relevant indicators [Tapiero 2008].

# Interaction with industry

The project adopted an exploratory, data-driven approach to identify real and potential insider threats for the chemical industry and methods to mitigate these security risks. It combined quantitative and qualitative methods, including scenario methods, semi-structured interviews, and participant observation. During the project, the two research teams met at repeated intervals to discuss tentative findings and further scope their research approach. Project methods and findings were presented and discussed at international academic fora, conferences and industry association meetings. The project teams engaged with a variety of international stakeholders, including policy and decision makers, regulators, industry managers, and employees.

The facilities visited, remain anonymous for the purpose of the study. They are geographically spread across Europe. Typically, one-day field visits, consisting of a joint session with several designated company members, one-on-one interviews with personnel, and “walkthroughs” - tours of industry infrastructures with managers and personnel took place. Thereafter follow-up exchanges, by email or phone.

The research yielded important insights and leads, which merit further consideration. Its value lies in its abductive ability to study security: Rather than starting from the theory of security, living definitions of key notions such as “barrier,” “security” and “insider threat,” were used with the aim of identifying patterns, trends, and relationships among data. These definitions were generated through interactions with research participants (industry). The observations, and inputs made based on interaction with industry made a pronounced impact on the development and drafting of the Handbook, which is to be used as a practically implementation tool to mitigate the insider risk. Further input was drawn from theories and academic concepts in order to merge the practical with the theoretical and develop a holistic approach to dealing with the insider threat.

## Analyzing Insider Threat through a Crime Theory lens

Crime theories offer a basis to explain insider behavior which focuses on the concept of opportunity and motivation: rational choice theory [Clarke 1997], routine activities theory, crime pattern theory [Cohen 1979] and situational crime theory [Hayward 2007].The situational crime theory has evolved most and includes the premise that the criminal might have access to the environment; a notion that goes hand in hand with the concept of the insider. In the light of situational crime prevention theory, some controls and measures that can be useful to address the insider threat are identified [Scott 2000]. The situational crime prevention theory identifies five categories for opportunity reduction measures:

1. Increase effort
2. Increase risk perception
3. Reduce rewards
4. Reduce provocation
	1. Reporting
5. Remove excuse
	1. Social responsibly

### Increase effort

This mechanismaims at stressing the perception that a specific crime would be difficult to execute. This can include target hardening, access control, exit interviews and screens, distracting or diverting offenders and potential offenders, to tools that can cause harm.

Figure 1. shows the effectiveness of the different policing strategies. The diagram shows that reliance on policing and law enforcement strategies or policies have limited effectiveness in curbing crimes or risks originating due to a problem (i.e. employee satisfaction).

#### Observations

The project team has found that the development of an effective security corporate strategy requires the involvement of the different stakeholders at different levels. The enforcement of rules might have adverse side effects and usually tends to have limited medium to long term efficacy in addressing internal risks in an organization (this can be observed in the three groups of culture outlined in the Handbook Section 4). Applying and developing policies alone is of limited effectiveness in addressing the insider risk, while developing a holistic culture and strategy backed up by mechanisms and measures can be of greater effectiveness. It was observed that companies with a clear committee / group or unit that tackles security risks and developed insider mitigation strategies are more open about sharing insider threat theft incidents. It was also clear that such companies have well defined incident and recruitment follow up procedures. Further, observations yielded that efforts in the direction of building sound security cultures in such companies was omnipresent. This was clear in the security awareness program for employees and the print outs that gave clear directions to the employees of how to act in case of emergencies. The leaflets focused on safety yet there were security elements. Further, the security committees tasked with insider threat in such companies seemed to have balanced representation from the different management backgrounds and employees. While companies who are less openly active about the threat did not share much details about historical incidents. While mentioning the incidents there was no clear set of procedures shared with the project team to reflect the post incident procedures or the mechanisms of how incidents took place. In addition, there was a higher level of centralization of responsibilities for the few persons responsible for the security aspects of organization and less diverse representation.

According to Jones and Colwill [Jones 2019] the isolation of vital and sensitive areas makes such areas more targetable and preferable targets for insiders. Porting that practice to chemical facilities would require following proper account policies and proper zone access program where employees have their responsibilities mapped in zones. It was observed that the companies applying access to zones are correlated to the existence of a security committee / unit / board responsible for the different aspect of security including insider threat.

While information control aims to divert offenders in the information technology field through honey pots[[6]](#footnote-6), key splitting[[7]](#footnote-7) segregation of duties and background checks of employees, similar techniques can be applied to chemical facilities to address insider threats. Similar to the *four-eye* principle in the nuclear field (also known as the two-man rule) chemical facilities can apply similar techniques where carrying out critical tasks requires that two individuals (who are less likely to collude or pose an insider threat) are to implement task around vital assets and sensitive areas. Both segregation of responsibilities and key splitting (four eyes) act as measures to prevent collusion and delay threat propagation. Prescreening for sensitive jobs is a measure usually implemented by the human resources department. Though enforcing the standard can be useful it might be of limited value according to [Pashalidis 2003] in predicting the future threat. The ISO/IEC 27002 [ISO/IEC 27002:2013 2019] offers several techniques for vetting the employees and offer background checks prior to employment. The controls are useful to offer a defined framework which employees should follow onsite. The framework can offer controls to ensure that the employees follow the security measures necessary to regulate access rights.

Applying the least privilege access control can be challenging due to overlapping responsibilities. However, access privilege can be associated with time validity based on the current needs. Regular audits are effective to identify and detect suspicious behaviors for users before the threat fully unfolds. Human resources ISO guidelines provides detailed directions on employee vetting and recruitment procedures [ISO/30405:2016 2019] which can be useful in avoiding recruitment of employees that have a potential to become insider threats in the future. For a detailed account on the procedure the reader is referred to [ISO/30405:2016 2019].



Figure 1 Effectiveness of policing strategies adapted from [Clarke 2005]

### Increase Risk Perception

This category involves improving detection mechanisms for breaches and threats and increasing the resistance to face maleficence [Scott 2000], for instance by extending guardianship, assisting natural surveillance, anonymity reduction, accountability, and by strengthening formal surveillance. However, excessive surveillance can result in an undesired opposite effect when people feel controlled, similar to the TSA case [Anteby 2019].

#### Observations

Some of the interviewees shared that the two person sign off rule was an effective measure to identify incidents that might require further follow up or can be suspected as insider theft incidents. However, no work has been carried out to assess the impact of the procedure on the trust mechanisms that will be discussed later in the report.

### Reduce Rewards

Reward reduction involves reducing the perception that execution of an insider crime is worthwhile [Scott 2000]. Target concealment is tricky when it comes to insiders, as in most cases the insider knows where the target (valuable asset) is located. However, knowledge on a need to know basis for sensitive targets can be an effective way to implement target concealment strategies. Compartmentalization can be an effective way of limiting the proper degree of access gradually, thus qualifying a smaller pool of people that have permission to be in the area, and thereby directly limiting the pool of potential insiders.

### Reduce Provocation

This category involves removing or neutralizing stimuli from the environment that may provoke insiders that are already motivated to commit offenses. The subcategories involved include frustration reduction mechanisms, avoiding disputes, reducing emotional arousal, and neutralizing peer pressure. The creation of a supportive working environment is an important mechanism to reduce frustration and stress which may act as motivators to the rise of insider malice. The categories above may include: the introduction of dispute resolution plans to contain and manage disputes effectively; discouraging imitation by ensuring a fix and return of the environment to what it used to be before an incident in case the incident introduces a change (fast clean up after evidence collection and prompt repair); support for whistleblowers; designing for natural surveillance to leverage concepts of bystander intervention, which have proven effective in dealing with sexual harassment [Schulte 2019], [Fischer 2011] and workplace or school bullying [Deutsch & Marcus 2011]. For a practical guide on reducing provocation and methods which could be applied please refer to section XXX of the Handbook.

### Reporting

Common in high-risk industries and most nuclear facilities [IAEA 2008], [IAEA 2013], the nuclear industry has developed internal incident reporting systems (IRS) with the aim of improving safety and security. These IRS are set up with the intention of gathering accounts of incidents, analyzing them, and ultimately, learning from them in order to avoid similar incidents in the future and the development of accidents caused by a cascade of incidents. To achieve this aim, employees are asked to feed inputs on real and potential incidents into the IRS and to share positive examples. Whereas companies can significantly benefit from having an IRS in place, it is crucial to understand whichincidents are reported and subsequently, whether or not, and how they are handled (Rossignol & Van Oudheusden 2016).

Incident reporting for the insider threat takes on a form distinct from other forms of reporting (e.g., safety reporting), as it draws attention to real or potentially deliberate and unauthorized acts against a company initiated by members of its own workforce. Discretion is therefore of utmost importance in identifying and documenting incidents. This can be facilitated by creating anonymous and codified mechanisms for reporting undesirable behaviour or suspicious behaviour. Whereas general features of the incident deserve to be shared with a wider range of audience to maximize learning, the specifics are only to be shared with a designated few. It is important to identify the learning objectives though it might not be possible to foresee all the consequences carried out by sharing information and incident details. An interesting case to learn from is the open source development in computer and information technology. In open source products, the code and the details of the application are open to the users. While open sourcing the code promotes flexibility and innovation, it also helps in discovering problematic areas and identifying backdoors in the system, or weak points. As a result, this might lead to a high number of security incidents reported when the system is released.

### Remove Excuses

This implies neutralizing the ‘rationalizations’ of undesirable activities of employees in the workplace by building a clear and distinct set of rules and procedures in the workplace. Crime perpetrators tend to justify their crimes. The mechanisms in this category include setting rules, posting instructions and ensuring there are standard procedures for the different activities. Assisting compliance, alerting conscience and controlling substance usage setting rules includes defining typical policies, agreements and procedures such as acceptable behaviors and usage of the premises and equipment. An assistive informative program could be developed to raise awareness on rules and procedures among employees [Hinduja 2013]. Promoting a healthy environment and ethically sound business practices constitute a strategy that supports the company with organizational policies and procedures which reduces the opportunity for individuals to get involved in criminal behavior and it helps define the normative behavior which is an important prerequisite to identify precursors of threats.

The mechanisms that can appeal to the user conscious include a code of ethics, warning messages and context aware spaces and interfaces. A context aware space (also called smart space) is an environment that has sensors which sense activities or actions or user states in order to offer services or support for the needs of the users. Smart or context aware environments heavily rely on a multitude of sensors and sensor networks that produce a large amount of data to be analyzed and reacted by the user or/and the systems/devices of the space [Pantsar 2010], [Saleemi 2011]. Context aware spaces and smart spaces can offer a transparent way to react to changes in an environment. Implementing these spaces can be costly but provide a return on investment if integrated in the culture of the company with the mindset to meet business needs and speed up meeting objectives.

### Social Responsibility

Following Burgess et al. [Burgess 2018] ,security policies can only be successful in the long run if the various social, ethical and ecological impacts, threats and opportunities, are assessed and prioritized alongside technical and commercial impacts. For the insider threat, a broader debate with all relevant stakeholders (industry players, regulators, decision makers, and others) is required as to what constitutes responsible organizational behavior and how such behavior may prevent and mitigate security risks in the immediate and long term. Examples from the project team's fieldwork underline the importance of engaging with the notion of social responsibility in security.

#### Observations

It was argued that a limited loss of chemical substances from the operating facility does not constitute a business risk. However, risk can be interpreted more broadly to encompass not only the immediate economic gain or loss for a company, but also how businesses are seen to adhere to social values and concerns, such as good stewardship (please refer to Handbook Section 4 on the three groups of safety and security culture and its impact to business processes).

**Limitations of the Crime Theory in Understanding the insider threat**

While the crime theory offers a great tool to dissect and understand the insider threat problem, a more holistic approach can help address the challenges motivations and conditions in an organization that might lead to the materialization of insider threat. Based on the work conducted and observations made; different aspects in the organizational culture might suppress or promote the materialization of insider threat events (please refer to Handbook Section 4.4 attributes of management and personnel behaviors). Crime theory is focused on the dynamics of the individual while organizational culture looks at the dynamics as a whole and its share in suppressing or promoting the materialization of insider threat. Crime theory emphases procedures and codes of conduct for the individual in addition to the conditions surrounding the perpetrator. While organizational culture includes focuses on the dynamics of the organization that might be enablers or disablers to the materialization of the insider threat. Further, organizational culture assesses the impact of barriers not only from the quantitative point of view in its ability to devour a malicious event or detect it but also the impact of the barrier on the culture and finally the business objectives in the corporate world. Thus, crime theory is a useful, albeit insufficient, lens to gauge insider threats in the chemical industry. The fieldwork highlights the importance of taking into account the broader context within which crimes and threats emanate, such as trust, organizational culture, data culture, behaviors and work environments. Subsequently, recommendations merging together insights from the literature and fieldwork are presented in order to ensure a holistic approach to insider threat mitigation with practical implementation measures to achieve insider mitigation described in more detail in the Handbook.

## Relevant Attributes and Dimensions of Insider Threat Analysis

Identification of minimum quantiles of chemical precursors that can be used for explosives proved ineffective in providing controls for theft risk. The main reason for this is the very low quantities of material is needed in order for those to be used as explosive precursors (e.g. in the 5 -15 kg range). Due to the production volumes of these precursors (in tons) it makes it very difficult to accurately account for quantities as low serval hundreds of grams or a few kilo grams.

As a result, there is a need for an integrated policy that spans not only the aspects covered by Crime Theory but also includes the following dimensions in an organization: trust and organizational culture (security culture, safety culture and data culture).

### Trust

During the interviews and the field the concept of trust has surfaced strongly. Most of the interviewed stakeholders confirmed that trust affects the dynamics of the interaction in the organization especially in terms of perceiving and dealing with insider threat. According to [Baracaldo & Joshi 2013] trust is a subjective expectation an agent has about another’s future behaviour based on the history of their encounters”. The definition acknowledges the subjectivity of trust and the dimension of perception which makes it challenging to quantify and assess. In addition, the definition puts a tricky condition to operationalize trust which is the history of encounters. It will be difficult to reach a trust estimate for an agent if there has not been a historical encounter. According to Finkel [Finkel 2019] and Pieters [Pieters 2011] trust is one of the skills that humans excel at which helped them dominate the planet by being able to trust in other humans whom they do not know. This ability supports effort scalability; as a result, a group of individuals can work to achieve a bigger goal that might not be achieved by each individual alone. As a result, the interaction of parts when combined produce a total effect greater than the sum of the individual elements.



Figure 2 A summary of the main trust attributes in an organizational context

Figure 2. defines the main attributes that can be used to reason about trust in an organizational context. The diagram offers a concise taxonomy to present a coherent set of concepts that are relevant to trust and impact the way trust is developed or eroded among employees. Figure 2 acts as a compact ontology, description of the concept of trust and the important connected concepts to trust in an organizational context. The importance of trust management stems from the need to cooperate and collaborate on tasks inside the organization. This affects how far managers or employees can take risks by involving others in tasks that requires collaboration. Contracts, regulations, rules, policy fall under the set of guidelines that can offer a mechanism that replaces trust when it is hard to establish. Although they are more likely to work and help in providing a basis to accomplish an interaction that relies on trust. However, the rules when relied on solely, might harm the organizational culture and could eventually result in the diffusion of distrust in the organization resulting in less loyalty among employees towards the organization. Rules, laws and internal policies should be used carefully in order to avoid the development of unhealthy culture. Adoption refers to chain of trust where a truster extends his/ her trust to another truster regarding a trustee (the practical implementation examples can be found in section 4.4 of the handbook dealing with management and personnel behaviors).

### Organizational Culture

The concept of organizational culture is one of the dimensions that shape the dynamics in an organization / company or facility. Awareness of organizational culture varies among different managers and companies. It is a challenge to ensure a high level of cultural awareness among employees to guide actions. It is paramount to pay attention to organizational culture as an enabling environment and set of driving forces for ensuring a positive operating state for the organization where it can guide the actions of employees and help manage the insider threat. The centrality of the culture concept follows from the shared meanings for an action in the organization. While the concept of organizational culture is viewed as a shared and learned set of experiences, meanings, values and understanding which inform and guide people while being expressed and communicated (The concept of organizational culture).

As a result, it is of an important value to understand and analyze organizational culture in the context of insider threat mitigation (Tools for spot checking culture and examples of prudent culture and behaviors which reduce the likelihood of an insider threat situation can be found in the Handbook Section 4, 5 and 6). Although barriers can act as quick fixes to address imminent threats and unfolding challenges long term effective solutions call for a thorough understanding of the forces and dynamics inside the organization.

Three relevant subcultures have been identified that are directly relevant to the analysis of the dynamics of insider threat:

* Security culture
* Safety culture
* Data and information culture

### Security Culture

While many researchers consider security culture in an organization important and crucial there has been little research in the area of identifying the dynamics of security culture for insider threat mitigation. Exploring the organizational culture is a prerequisite to understanding the dynamics and developing an effective insider threat mitigation program. The project team developed nine attributes based on the framework introduced by Detert [Detert 2000] to analyse organizational security culture based on the field work and group interviews. The attributes can guide the work necessary to understand and improve security culture in an organization or facility which can be carried out through surveying, polls, interviews and inspections (a practical implementation guide for spot checks can be found in the Handbook section 5). The following are nine factors based on Detert study that an organization could use to analyze their security culture:

**1-Basis of truth and rationality**

This attribute focuses on understanding what is real inside an organization and devising methods to understanding what is true. This may affect the degree of adopting of normative or pragmatic attitudes of employees in an organization towards security.

**2-The time horizon**

The time horizon dimension aims to discover whether the organization is adopting only short-term ad hoc needs or there are also a long-term strategy goal setting strategy from the leaders and the management in the organization

**3-Motivation**

Motivation dynamics of employees and organizations need to be identified which include the motivating forces.

**4-Stability versus change/ innovation / personal growth**

Some organizations and individuals are open to change while others have a low tolerance for disruption. Risk taking organizations tend to be innovative with a mindset of pushing the constant and are involved in continuous improvement. While risk averse organizations tend to focus on stability and on avoiding actions or initiatives that might disrupt the status quo.

**5-Orientation to work, task and co-workers**

While work is an important economic activity, it is usually compared to social activity. Some organizations look at work as a task-based activity concerned with accomplishments and productivity while others focus on the comfort of, and the balance of, employee life where higher levels of employee satisfaction and organizational achievements are sought. Key observations during field visits were the dominance in some organization placed on knowing each other and the mutual trust. Although the notion of trust in individuals acts as a social currency in the organizational culture it is important to move the trust from blind trust to evidence-driven trust.

**6-Isolation versus collaboration and cooperation**

Underlying beliefs of the nature of human relation and their impact on work accomplishment whether it is individualism, collaboration or cooperation.

**7-Control, coordination and responsibility**

Organizations vary in the degree of centralization of responsibility concentrated or shared. When control is tight there are formal rules, procedures and guidelines that are set by a few (management) to guide the behavior of the majority of employees. A loose control offers flexibility and autonomy with few written rules and formal procedures, while a shared environment of decision making and learning becomes a promoting environment to carry out the different tasks expected from employees.

**8-Orientation and focus- Internal and /or external**

The organization may have an internal orientation focusing on people and processes within the organization or external orientation focusing on external driving forces such as customers competitors and the environment. The organization might have an internal orientation where they focus on employees, their productivity. These orientations are complementary. For instance, one research participant stressed that in the supply chain, farmers are “insiders” rather than outsiders.

**9-Proactivity versus reactivity**

A ninth dimension was added that the project team perceive as important in the ability of an organization to respond to security risks and increase robustness of the culture to respond to insider threats: reactivity and proactivity. These are two approaches of handling risks and perceiving the environment where the first focuses on setting up approaches to perceive evolving situations. In addition, the speed of reacting towards accidents and incidents might disrupt the business needs.

### Safety culture

It can be noticed that most aspects of safety culture such as characteristics and attitudes in in the organization are of intangible nature and can be evaluated only indirectly, by looking at the tangible manifestations they generate [IAEA]. Given its complexity, safety culture assessment requires multiple data collection methods, among which document reviews, observations, focus groups, interviews, audits, expert evaluations and questionnaires [Guldenmund 2000] (these are contained for practical implementation in the Handbook Section 5). Another aspect worth investigating is the integration of safety and security culture with the support of evidence-based recommendations to carry out the needed changes to the organization (namely corrective actions). Some facilities visited seem more ready to carry out the integration between safety security and evidence driven recommendation due to the presence of mechanisms that support data collection and analysis in the organization. While others interviewed would benefit from a gradual introduction and building approach for the safety and security auditing (please refer to Sections 4, 5, and 6 of the Handbook). Forming a team from different members in the company whose aim is to identify relevant safety and security aspects and use one of the existing frameworks to carry out the assessment would be a beneficial strategy (please refer to the Resources section of this document).

### Data culture

Data culture is the principle that requires staff, employees and decision makers to focus on information conveyed by the existing data. Decisions and changes are driven and backed up by evidence and data in addition to experience instead of decisions based on rules of thumb or experience solely. Analyzing insider threat properly requires enabling mechanisms that can capture relevant data and help analyze it. This can include logging systems, surveillance zones and analytics dashboards which can in real time show potential threats to vital areas. However, it is important to ensure that the surveillance and the data culture does not become a coercive culture with the excuse of curbing insider threat [Underwood 2019].

In order to enable data collection for the different phases of chain supply, a good place to start is through the development of material accountancy approaches. It was observed that some facilities have active dashboards that can be used to monitoring active risks in safety. The same concept can be applied to support actively addressing security risks by building safety and security dashboards which can visually represent the level of danger or risk in a zone. In order to develop such a tool, the needs of the organization need to be analyzed in addition to the risks (for some highlights of guiding questions that can be useful in developing such an approach please refer to Handbook section 7, 8 and 9). Depending on the needs of the organization it might make more effective to develop either unified dashboards that can fuse security and safety or separate ones.

Some of the visited facilities shared how they approached digitization efforts. While they said that the digitization efforts for storage facilities were useful the initiative was aborted after one year of implementation. The interviewers have not shared details on the challenges faced yet they stressed the fact that they would like to come back to the initiative and role it one a wider scale. We observed that digitization is a challenging tricky process which usually requires slow steps towards digitization of the supply chain. Nicolas Windpassinger (Digitize or die) outlines a five-step process to digitize facilities While digitizing a business or company is a challenging task, taking small steps that are tied with the business goals and aligned with the organization culture can pay off [Windpassinger 2017]. Building a data culture can be an initial step towards digitization. This can start by identifying opportunities through two steps: supporting operations with data insights and promoting a data learning environment.

# Barrier Selection and Adoption

During the technical visits observations were made of the different barriers facilities adopted in context to their security plans. During the interview’s reasons given for barrier selection were not always clear. A structured approach to barrier selection and its usefulness in terms of mitigating the insider threat can be achieved by utilizing the Handbook Section 8. Interviewees did not share their approaches for barrier selection, this could be perhaps due to the absence of a formal objective method to choose barriers or due to confidentiality needs.

Barriers can act as an effective approach to delay detect, deter and even aid with the repose of a perpetrator from materializing an insider threat. However, an objective set of criteria needs to be applied in order to ensure an effective approach in selection deployment and operation of the barrier. We classified barriers into two groups:

* Soft barriers: The mechanisms and policies both implicit or explicit in the organization that can impact the mitigation or insider threat. The soft barriers include the organizational culture and policies which might act as an enabler or disabler for risks. An example could include the organizational culture with its subcultures.
* Hard barriers: The devices, systems or procedures that can be used, installed or developed to delay, detect or deter. An example of that could include cameras and access control mechanisms.

Kiszelewska presented a set of criteria relevant to the selection of the safety and security of physical space [Kiszelewska 2013]. Based the field work the project team extended Kiszelewska’s work and developed a relevant set of attributes that can guide an organization to reason and rank the different measures available to mitigate relevant risks. Figure 3 presents the main relevant attributes that can help an organization pick a barrier to address a specific phase of the risk. It can also help reason the suitability of the barrier and its compliance to different policies or laws of the country.

****

Figure 3 Relevant barrier Selection Factors

There are two main approaches to reason about the suitability of the barriers: quantitative or qualitative. Different Multi Criteria Decision Analysis (MCDA) techniques can be applied to fuse the values for the attributes identified; we refer to [Brans 2005]. The attributes defined can work as the basis for a decision support system that can offer insights on the most suitable set of attributes to mitigate the risks of a scenario. From our observations we identified multiple barriers per facility that seem to provide and to the concepts of in depth researched in [Khakzad 2011] one or more of the 5D framework presented (deter, deny, detect, delay and defend). For more details on adversary sequence interruption (EASI method), or the systematic analysis of vulnerability to intrusion (SAVI method) we refer the reader to [Argenti 2017].

# Limitations

This section discusses the types of limitations faced while carrying out the research in the study. It is important to be aware of the limitations in order to properly benefit from the findings and recommendations included in the current report.

1. **Sample Size**

This project is a first-of-its-kind qualitative explorative research study which is non exhaustive for all the facilities across Europe. As a result, the findings should not be generalized across the chemical sector and the special conditions and circumstances of each facility should be considered. However, as we note above a single actor or event can have significant impact on safety and security.

1. **Lack of available and/or reliable data and prior research studies on the topic**

The work started by looking for studies that present and define insider threats in chemical facilities. The project team was not able to locate rigorous work that tackles, defines or lists insider threat incidents. The sensitivity of the topic for the different companies and facilities involved, made it difficult at times to locate some of the incidents that made their way to public journalism outlets, with the assumption that perhaps there might have been more than what makes its way to conventional outlets. The situation puts a challenge to analyze events that can benefit others and act as a collective learning opportunity.

1. **Self-reported data**

A significant portion of the data collected and analyzed in this research study relied on what research participants were willing and able to share. There is ambiguity within and across organizations in how the mechanisms motivating security implementation are, or should be, deployed. While there is no reason to assume that participants were untruthful when conveying information, they may not have disclosed all information for various reasons.

1. **Exaggeration**

Several research participants in different companies stressed that employees within their organization “fully trust” one another and that this trust is created and sustained through day-to-day social interactions. This claim, while widely shared, is not always based on compelling arguments, or existing research and evidence. Insiders may be highly trusted and sociable individuals. Furthermore, trust is built by establishing durable relationships between all stakeholders, including employers and employees, staff and customers, internal stakeholders and external clients. It is also important to consider how trust is mediated through technologies and procedures. To give an example, some may see surveillance cameras as beneficial to establishing trust, others as detrimental to that same aim.

1. **Access**

Gaining access to the field and establishing mutual trust to discuss security breaches and/or vulnerabilities has been a challenge that the project team believes to have overcome. However, there was limited engagement from a wide range of employees “on the ground,”; these perspectives are missing from the current study.

# Recommendations

These recommendations are based on a combination of lesson learnt from the fieldwork undertaken as well as theoretical concepts, and experiences from other comparable strategic industries. They are meant to sensitize stakeholders to the insider threat and offer guidelines on how to manage it effectively, without compromising company procedures and workflows. Each recommendation is followed by a section title, where more information on the topic at hand can be found. This coupled with the Handbook containing smart measures allows for a holistic approach to insider threat mitigation for chemical precursors to explosives.

1. **Make mitigating the insider threat an integral part of the corporate security culture.**

Ensuring that there is an incident reporting system for security, through active security training for employees, and by creating a culture that supports bystander participation and intervention in the case of incidents. An internal customised regular risk assessment policy is needed that includes a wide variety of stakeholders in the company, using for example *what if* scenarios, fish diagrams, hazard detection methods as guiding tools.

1. **Trust but verify.**

Build informed trust circles by enabling and supporting accountable actions. To promote accountability, the organisation needs to ensure an access system that can be traceable (for example map of zones, assets and actions to employees). Active auditing and the development of warning signals are critical to recognizing threats at an early stage. The warning protocol can be manual or it can include technological approaches such as automated monitoring systems. Early warning systems should be taken cautiously and seen as assistive, investigative tools rather than end decisions. Ensure the right balance between monitoring and access control mechanisms and freedom and flexibility of the employees. Check the regulation for information collection before developing of early warning systems. For more information and practical approaches to leadership and organizational models please refer the handbook.

1. **Build a supporting organizational culture**.

Link safety, security and data driven culture with the with long-term learning and organizational objectives. Improve public perception by taking social responsibility projecting an active image towards society will ensure that organizational branding can affect loyalty and perception of employees and society. Develop ethics codes and carry out awareness campaigns

1. **Accept the insider threat.**

A strong security culture cannot take hold within an organization unless appropriate security behaviors, attitudes, and assets are identified, considered, and regularly rehearsed with the input of all stakeholders. To facilitate the development of such a culture, acceptance that insider threats do occur and have severe consequences is necessary.

1. **Sustain an inquisitive attitude centered on learning about security (including insider threats.)**

Asking regularly how security culture can be improved. Questions worth asking time and again are: Where can we improve? Where do we fall short? What are we missing here? It is about developing a culture in which all are actively curious about their blind spots.

1. **Tailor insider threat mitigation to address the specific needs and concerns of the organization.**

Whereas it is possible to agree on general principles and approaches, security programs vary across domains, organizations, and cultures. Delving into the organizational, technical, and cultural specifics of security is a necessary, albeit insufficient, step towards managing security for a particular organization. In the Handbook several barriers are described from the perspective of standalones and the measures which would be required in order to compliment those, these can provide guidance and what system might be applicable to the individual organizations security system to mitigate the insider threat.

# Resources

Following is a list of resources and key documents useful for Implementing guidelines to curb insider threat.

* ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls.
* 20 Practice steps for mitigating insider threats: Carnegie Mellon Guide to Mitigating Insider Threat
* ISO 30405:2016 Guidelines for recruitment
* ISO 30414:2018 Human resources management guidelines for internal and external human capital reporting
* NIST (National institute of standards and technology) Guidelines Insider threat mitigation
* DHS (The Department of Homeland Security) national plans for critical infrastructure insider
* Iso Physical security 27001 how to protect secure areas
* ISO SEC 27032 Cybersecurity
* ISO SEC 27001 information security
* ISO, 2006, ISO 26000: Guidance on Social Responsibility
* Fertiliser Industry Assurance Scheme [https://www.aictradeassurance.org.uk](https://www.aictradeassurance.org.uk/)
* Chemical Sector Security Awareness Guide <https://www.dhs.gov/sites/default/files/publications/DHS-Chemical-Sector-Security-Guide-Sept-2012-508.pdf>

# Conclusion

While in organizations, insider threats tend to be managed through security related activities, long-term, holistic mitigation strategies are needed. It is crucial to realize that the risk exists with the organization and that carrying out preparedness activities and risk assessment is a continuous activity that needs to take into account business needs, organizational culture, stakeholder expectations and technological evolutions. Solutions need full integration and support from the different organizational layers to succeed and yield the most optimal results. Building trust and loyalty among employees can be a crucial security net an organization could rely on in addition to physical barriers that should be in place. Tailored methodologies to assess different dimensions of organizational culture are necessary to guide the activities in security, safety and digitization efforts. Responsible and accountable monitoring systems can support enabling and learning organizations where the employees are trusted while being held accountable to their actions. A learning culture helps shape the security needs of the organization and helps the organization respond in a flexible manner to arising risks and opportunities. For future research the project team would like to expand the definition of an insider to include systems that operate internally or are relied upon by the facility, factory, or organization that can result in consequential damage or can support the intentions and damaging acts of an insider.

Subsequently, the project team initiated cross-case comparison to give a sense of real and potential security challenges across organizations (horizontal matching), and link common evidence of challenges and issues to specific, situated experiences (vertical matching). Thus, the aim was not to provide an exhaustive overview of how security is enacted in the chemical industry at large but to open a space for informed dialogue and mutual learning by tapping into examples and challenges and testing theories. The scenarios as well as the proposed measures, and tools were derived from other critical industries and experts’ experiences. Research work has been carried out to identify internal vulnerabilities in systems which can benefit in auditing the vulnerabilities of such systems, especially information-based infrastructure. Thus, the definition of insider should extend beyond the human actor and beyond spatial-temporal characteristics.

# References

1. Argenti, Francesca, et al. Security risk assessment: in the chemical and process industry. Vol. 1. Walter de Gruyter GmbH & Co KG, 2017.
2. B.R. Munier and C. Tapiero, Risk attitudes, in: Encyclopedia of Quantitative Risk Assessment and Analysis, Wiley, New York, 2008
3. Baracaldo, N., & Joshi, J. (2013). An adaptive risk management and access control framework to mitigate insider threats. Computers & Security, 39, 237-254.
4. Baracaldo, N., & Joshi, J. (2015). An adaptive risk management and access control framework to mitigate insider threats. Computers & Security, 39, 237-254.
5. Baracaldo, Nathalie, and James Joshi. "An adaptive risk management and access control framework to mitigate insider threats." Computers & Security 39 (2013): 237-254.
6. Brans, Jean-Pierre, and Bertrand Mareschal. "Multiple criteria decision analysis: state of the art surveys." PROMETHEE method (2005): 200-232.
7. Brigid Schulte To Combat Harassment, More Companies Should Try Bystander Training
8. Catrinel Turcanu, Lusine Mkrtchyan, Ahmed Nagy, and Pierre Faure. 2015. Can belief structures improve our understanding of safety climate survey data?. Int. J. Approx. Reasoning 66, C (November 2015), 103-118. DOI: https://doi.org/10.1016/j.ijar.2015.08.005
9. Celikel, E., Kantarcioglu, M., Thuraisingham, B., & Bertino, E. (2009). A risk management approach to RBAC. Risk and Decision Analysis, 1(1), 21-33.
10. Clarke, R. V., & Eck, J. E. (2005). Crime analysis for problem solvers in 60 small steps. Washington, DC: US Department of Justice, Office of Community Oriented Policing Services.
11. Clarke, Ronald R. (ed.) (1997). Situational Crime Prevention: Successful Case Studies. Second Edition. New York: Harrow and Heston. ISBN 0-911577-39-4
12. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American sociological review, 588-608.
13. Cole, Eric, and Sandra Ring. Insider threat: Protecting the enterprise from sabotage, spying, and theft. Elsevier, 2005.
14. Database of CBRN terrorism by non-state actors: START https://www.start.umd.edu/gtd/

1. Detert, James R., Roger G. Schroeder, and John J. Mauriel. "A framework for linking culture and improvement initiatives in organizations." Academy of management Review 25.4 (2000): 850-863.
2. Deutsch, M., Coleman, P. T., & Marcus, E. C. (Eds.). (2011). The handbook of conflict resolution: Theory and practice. John Wiley & Sons. Last accessed https://www.wiley.com/WileyCDA/Section/id-818315.html 12 March 2019.
3. F.W. Guldenmund, The nature of safety culture: a review of theory and research, Saf. Sci. 34 (1) (2000) 215–257.
4. Finkel Alan. World Economic Forum What will it take for us to trust AI?" published 12 May 2018 last accessed 4th May 2019 Accessed at: https://www.weforum.org/agenda/2018/05/alan-finkel-turing-certificate-ai-trust-robot/
5. Fischer, Peter, et al. "The bystander-effect: A meta-analytic review on bystander intervention in dangerous and non-dangerous emergencies." Psychological bulletin 137.4 (2011): 517.
6. Hayward, K. (2007). Situational crime prevention and its discontents: rational choice theory versus the ‘culture of now’. Social Policy & Administration, 41(3), 232-250.
7. Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. Security journal, 26(4), 383-402.
8. IAEA, Safety culture, Safety Series No. 75-INSAG-4, International Atomic Energy Agency, Vienna, Austria.
9. INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, Technical Guidance No. 16, IAEA, Vienna (2013).
10. INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, Implementing Guides No. 8, IAEA, Vienna (2008).
11. INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, Implementing Guides No. 8, IAEA, Vienna (2008).
12. ISO/30405:2016 Human resource management -- Guidelines on recruitment last accessed 11 March 2019.
13. ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls (second edition) last accessed 11 March 2019.
14. Jones, Andy & Colwill, Carl. (2019). Dealing with the Malicious Insider. Australian Information Security Management Conference.
15. Khakzad, Nima, Faisal Khan, and Paul Amyotte. "Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches." Reliability Engineering & System Safety 96.8 (2011): 925-932.
16. Kiszelewska, Agnieszka, and Michael Coole. "Physical security barrier selection: a decision support analysis." (2013).
17. Last accessed https://hbr.org/2018/10/to-combat-harassment-more-companies-should-try-bystander-training. 12th March 2019
18. Michel Anteby and Curtis K. Chan Harvard business review. Why Monitoring Your Employees’ Behavior Can Backfire APRIL 25, 2019 https://hbr.org/2018/04/why-monitoring-your-employees-behavior-can-backfire
19. Mohsin Saleemi, M & Diaz Rodriguez, Natalia & Lilius, Johan & Porres, Ivan. (2011). A Framework for Context-Aware Applications for Smart Spaces. 6869. 14-25. 10.1109/SAINT.2011.39.
20. National Academies of Sciences, Engineering, and Medicine. 2018. Reducing the Threat of Improvised Explosive Device Attacks by Restricting Access to Explosive Precursor Chemicals. Washington, DC: The National Academies Press. https://doi.org/10.17226/24862 Chapter 4
21. Newton, K., Stolle, D., & Zmerli, S. (2018). Social and political trust. The Oxford Handbook of Social and Political Trust, 37.
22. Pantsar-Syväniemi, S., Simula, K., & Ovaska, E. (2010, June). Context-awareness in smart spaces. In The IEEE symposium on Computers and Communications (pp. 1023-1028). IEEE.
23. Pashalidis, A., & Mitchell, C. J. (2003, July). A taxonomy of single sign-on systems. In Australasian Conference on Information Security and Privacy (pp. 249-264). Springer, Berlin, Heidelberg.
24. Pieters, Wolter. "Explanation and trust: what to tell the user in security and AI?." Ethics and information technology 13.1 (2011): 53-64.
25. Sarah Underwood. 2019. The fine line between coercion and care. Commun. ACM 62, 4 (March 2019), 15-15. DOI: https://doi.org/10.1145/3311721
26. Scott, J. (2000). Rational choice theory. Understanding contemporary society: Theories of the present, 129, 671-85.
27. Windpassinger, Nicolas, and Jean-Pascal Tricoire. Digitize Or Die: Transform Your Organization, Embrace the Digital Evolution, Rise Above the Competition. IoT Hub, 2017.
1. Database of CBRN terrorism by non-state actors: START https://www.start.umd.edu/gtd/ [↑](#footnote-ref-1)
2. National Academies of Sciences, Engineering, and Medicine. 2018. Reducing the Threat of Improvised Explosive Device Attacks by Restricting Access to Explosive Precursor Chemicals. Washington, DC: The National Academies Press. https://doi.org/10.17226/24862 Chapter 4 [↑](#footnote-ref-2)
3. For more quantitative calculations, consult the Sadovsky Formulas; http://www.sciencemadness.org/talk/viewthread.php?tid=15150&page=2#pid197153 [↑](#footnote-ref-3)
4. This project builds on the IAEA definition of ‘insider’. Nuclear facilities and nuclear transport have been substituted by chemical facilities and chemical transport (IAEA Preventive and Protective measures against insider guide INFCIRC/225/Rev.5 IAEA Nuclear Security Series No. 13). [↑](#footnote-ref-4)
5. Developing a Security Culture Last Accessed: https://www.cpni.gov.uk/developing-security-culture [↑](#footnote-ref-5)
6. In computer terminology, a honeypot is a security mechanism set to detect, deflect, unauthorized use of information systems through deception of perpetrators. Honeypot consists of data assets that appears to be a legitimate part of a system, but is actually isolated and monitored which seems to contain information or a resource of value to attackers / insiders. The approach is similar to police sting operations, coined as "baiting," a suspect. However, honeypots provide an important mechanism to delaying the attack process of a perpetrator to the system and waste their time and resources. Similar mechanisms can be developed for mitigating insider threat. (Spitzner, L. (2002)). [↑](#footnote-ref-6)
7. Key splitting refers to methods for distributing parts of a secret key in amongst a group of participants, each of whom is allocated a share of the secret key. To access the secret and reconstruct the information a sufficient number of participants have to combine their secret key parts; individual shares are of no use on their own.Michael O. Rabin. 1989. Efficient dispersal of information for security, load balancing, and fault tolerance. J. ACM 36, 2 (April 1989), 335-348. DOI: https://doi.org/10.1145/62044.62050 [↑](#footnote-ref-7)