HOW TO REACT ON SIGNS OF CHANGES IN BEHAVIOUR THAT MIGHT BE SIGNES OF CONCERN?

Lisa De Laet
FANC
Brussels, Belgium
Lisa.delaet@fanc.fgov.be

Christelle Creus
FANC
Brussels, Belgium

Rony Dresselaers
FANC
Brussels, Belgium

Tony Snoeck
FANC
Brussels, Belgium

ABSTRACT

In many countries there is some sort of screening in place as a preventive mitigation tool against the insider threat. A screening however, provides a picture of a person at a specific moment in time, based on the information that is gathered. Even though these screenings are conducted on a regular basis, it is still necessary to have some sort of follow up of these people who are working with sensitive material or sensitive information. A screening provides an overview of the past of someone, which we accept as an indication of behaviour in the future. In Belgium, to have a concrete case, we have a security officer who will be responsible for demands of screenings and to follow up the people who are screened. It is however very difficult to have one person who is responsible for everyone in a facility. There should be a system in place where signs of changing of behaviour can be signalled in order to react. In this setting it is important to define a baseline of behaviour. Without this baseline, you cannot define a change in behaviour. The difficulty is that every person is different and thus it is impossible to have a basic baseline and in cannot really be done by someone who is not in regular contact with the person him- or herself. It is therefore very important to identify the specific functions or people who are in the possibility to have this base of behaviour and can identify change. During the international Symposium on Insider Threat Mitigation in March 2019 we have done an exercise on this topic. During this interactive session, we set out a specific profile and indicated a 'baseline behaviour'. Based on indicated signs of changes in behaviour we challenged the group to think about when and how they would react. During this exercise, with a sample of people working on insider threat, it was clear that it is a difficult balance on when to react. In general, one small difference in behaviour did not trigger any concrete reaction. Nevertheless when we put different small pieces of information together, most participants indicated they wanted to react. The different pieces of this new picture came from different parts of the facility: colleagues, HR service, line manager,… This is not information that is always brought together, which adds to the challenges of this subject. The reaction and the way it was conducted depends strongly on the legislative options and of the culture of the country, the company and the security culture. In aftercare, it is a challenge to have concrete guidance, mainly because it depends so much on the legal possibilities and the culture. It is however clear that there needs to be some sort of system in order to follow up people who have been screened and that it needs to take into account different partners in the facility. In the paper we would like to address these challenges and look and the different roles and responsibilities to report in an aftercare system.

1. INTRODUCTION

In many countries there is some sort of screening in place as a preventive mitigation tool against the insider threat. A screening however, provides a picture of a person at a specific moment in time, based on the information that is gathered. Even though these screenings are conducted on a regular basis, it is still necessary to have some sort of follow-up of these people who are working with sensitive material or sensitive information. A screening provides an overview of the past of someone, which we accept as an indication of behaviour in the future, but it is obviously not a guarantee.

In Belgium, to have a concrete case, we have a security officer who will be responsible for the requests of screenings and to follow up the people who are screened, what we call 'Aftercare'. It is however difficult to have one or two people who are responsible for everyone in a facility. Moreover, because in the nuclear industry it is common to work with many different subcontractors, who are under the responsibility of another firm. Therefore, there should be a system in place to help the security officers conduct the aftercare and address signs of changes in behaviour that could lead to concerning acts that could be problematic. The information should be provided bottom-up to the security officer, so he can interpret and do some research if necessary and take concrete action.

When asking everyone in a facility to look out for signs, it is necessary to provide guidance. In this setting you are looking at human behaviour and at many different personalities. In order to identify changes in a person's behaviour, you need to define a baseline for his/her behaviour. Without this baseline, you cannot define a change. It is therefore important to identify the specific functions or people who are in the possibility to have this view on the people in the field.

In aftercare, it is a challenge to have concrete general guidance, mainly because the guidance is dependent on the legal possibilities and the culture of the country and of the facility. It is however clear that there needs to be some sort of system in place in order to follow up people who have been screened and that it needs to take into account different partners inside and outside the facility. In this paper we would like to address these challenges and look at the different roles and responsibilities to report in an aftercare system.

2. EXERCISE IN THE FIELD

To challenge these questions, we have conducted an exercise during the international Symposium on Insider Threat Mitigation in March 2019 and during the IAEA Advanced Course on Insider Threat Mitigations in July 2019. During these interactive sessions, we set out a specific profile and indicated a 'baseline behaviour'. Based on indicated signs of changes in behaviour we challenged the group to think about when and how they would react.

During this exercise, with a sample of people working on insider threat, it was clear that it is a difficult balance on when to react and how to react proportionally. It was however interesting to see that there was a difference in reaction between a group that was mainly working for regulators (International Symposium) and a group that was mainly working for the operator (IAEA course). In general, looking at the sample of people from the regulatory side, one small difference in behaviour did not trigger any concrete reaction. Nevertheless, when we put different small pieces of information together, most participants indicated they wanted to react by talking with the person him- or herself. Looking at the operators, they decided very soon, almost from the first sign, that a reaction was needed and indicated that they would have at least a conversation with the person in order to decide if they would take it up further. It is clearly useful to have a system in place to put different pieces of the picture together, so in case you hesitate to talk to a person, you might be in the possibility to look for further signs.

In both groups they decided at a certain point that they would react. However, it is clear that what they would and could do depends strongly on their specific legislative options and on the culture of the country, the company and the security culture in general. There is a difference in approach as to who has the responsibility to handle the signs of concerns, who would be best placed in an organisation and most definitely how they would address such a sensible issue. These are aspects that should be adapted to the facility.

3. PREVENTION

Anyone in an organisation can become an insider and radicalise in a certain idea or can be persuaded to do something. In the last couple of years we have seen a shift, where people radicalise on themselves through reading on the internet instead of participating in groups or organisations. Self-radicalisation is much more subtle as their actions are generally online and much more anonymous.

There are three levels of prevention in this area: the first level is to limit the risk factors, the second level is to identify the people at risk based on their behaviour and the third level is to discourage the possible thought of action against the organisation.

The first level of prevention looks at the limitation of the attributes of an insider. This means that a facility should minimise the access, authority and knowledge of an employee as much as possible. This obviously is dependent on the function of the person. Nevertheless, it is not always easy, as access, authority and knowledge are also necessary in order to conduct their function. It is however important to compartmentalise certain areas as well as documents and information on for instance security measures. This is a way to already minimise access to and knowledge of specific parts. This should also be taken into account when a person changes functions or workplaces and the access of employees should be regularly revaluated.

In order to identify the second level of prevention, you need to have an overview of the people in your facility and their access, authority and knowledge. You should also take into account the history of the person in the facility, as (s)he may have accumulated access or knowledge on the facility of previous employments. By identifying the people who have the most access, authority and knowledge, or those who have these attributes on critical parts of the facility, you have an overview of the people that could be more of a threat to the facility if they would become an insider. It is useful to have this overview to identify the people that should be observed more closely. This could also help during the analysis of reported aspects, as you can immediately take into account what the person is capable of doing.

With the third level of prevention we are looking at the discouragement of an action. This can be in various ways: people can be discouraged by the notion that they will get caught, for instance, but also by making the employees feel part of the organisation. In order to conduct an act against your employer there is often an aspect of disloyalty to the employer and maybe even disgruntlement as well. In order to prevent people from becoming an insider, they should be handled correctly and should feel appreciated for the work they are doing, so they don't want to do anything against the facility.

4. DETECTION: REPORTING SYSTEM

Next to preventions it is necessary to have detection of an insider. Next to technical measures to detect an insider act is happening, we should try to identify the intention and thus detect the indicators of a person who might be becoming an insider. The sooner the indication of someone who might want to do an insider act is handled, the smaller the risk that an act will be conducted.

Reporting is an important part of the insider threat mitigation program and comes back to the aspect of 'See something, say something'. The difficulty in reporting human behaviour is that it is always subjective, as it is an interpretation of a situation. Moreover, in the nuclear sector we are mainly working with engineers and technicians, who are generally not trained in addressing human behaviour. It is therefore important that there is a reporting system that is easily accessible and ensures that something is being done with the information that is given. This reporting system must be open to anyone in the facility, also subcontractors. To encourage the people that are reporting, education must be given on reporting, in order to signalise that everyone has a role in the organisation to be aware of potential issues and that they should use their common sense in order to report.

In general, reporting is seen as something bad. It can be perceived as 'tattling on a co-worker'. This is why most of the information is not being brought up. Information between co-workers is often shared because they trust each other, as you are working together and spend most of your days at the workplace. By reporting the information that is gathered during this working relationship, you seem to be breaking this trust. Nevertheless,

research has shown that often in insider cases, co-workers had their suspicions but did not report them. This allows the individual to continue their damaging behaviour much longer than necessary before they are stopped. There must be a clear procedure for reporting and it must be clarified that by reporting this behaviour, there is a possibility to help the individual. Generally, insider cases are linked to a personal problem or crisis. By identifying and addressing it, the person can be helped before turning to a malicious act.

The information however should also be checked, as it is subjective and the system could for instance also be misused to bring a person in discredit. Moreover, we cannot expect everyone to be a behavioural observation specialist or a security specialist, nor can we expect everyone to do their own investigation. This situation would create an atmosphere of dilation in the facility and may make it more difficult to work on an individual in the process of radicalisation or a radicalised individual. It is therefore important that the information can be caught as 'raw material' and that it can be looked at by people with proper skills and means who can verify the information and bring it together with possible other signs.

5. SECURITY CULTURE

Having a reporting mechanism and a mechanism to get information to the relevant security officers in order to address it, is key in behavioural observation. Having a culture where reporting is imbedded, will help identifying changes in behaviour and security concerns which might identify a possible insider. Moreover, it can also serve as a 'demotivational' system, as a perpetrator might be more reluctant knowing he can be caught.

Culture in itself can be defined as 'the ideas, customs and values of a particular group'. Ideally, everyone in the facility should have a sense of the same ideas, customs and values in order to react to situations that are against these values. Everyone must be aware of the rules and procedures and of the aspects of the insider threat, otherwise they will not report these issues. Every employee should be formed, in order to educate personnel on the subject and it is useful to look at the analyses of the access, authority and knowledge of everyone (as explained in point 3). The people who pose the biggest risk to an organisation, should have a higher awareness, as they should be looked at more closely.

Working on a strong security culture is important in an insider threat mitigation program. As this is your basis for reporting signs of concern.

6. DEFINE A BASELINE

In order to report a change in behaviour you need to be in regular contact with the person him- or herself. You must be able to analyse if the action of the person is a change in general or just a one-time action. Overreporting on every person who has a bad day, can clutter the reporting system and take the focus away from those reports that are actually necessary to look at.

In order to see changes in behaviour you need to know if a certain behaviour is normal for a person or not, for example: we can have a person who from the moment (s)he is agitated starts yelling at everyone. If we see this person yelling at someone, we can assume it is because this person always does this. We can also have a person who barely raises his/her voice in an argument, if we see this person yelling at someone, you can assume something is wrong.

Moreover, an additional part to focus on is to identify security and safety issues. A person who violates security or safety rules is a bigger risk to becoming an insider. In order to identify these issues, you need to have clear and practical rules and procedures that are known in the facility and are followed. This is an aspect that can be measured and noted, it goes together with a good safety and security culture, because if the culture to follow these rules is not there, no-one will notice if there is a safety or security violation. Moreover, no-one will report the violations.

This means that everyone in a facility will need to be aware that a change in behaviour shouldn't be left

unreported. The only people who will be in the possibility to define a baseline in behaviour are these people who work together. The culture in the company and the openness to the line manager or other roles in the facility (such as HR) are key aspects in this area. Employees should be able to feel at ease when talking about concerns about a co-worker. They should be in the possibility to address these issues and talk about it, without it being perceived as a unusual or suspicious event.

7. IDENTIFY SPECIFIC FUNCTIONS AND PARTNERS

In most cases of insiders, there were more than one sign of concern (behavioural, security concern, ...) before the criminal act itself. It is therefore necessary to identify and capture these signs. These are not only signs that are seen by the closest co-workers, but should also be picked up by security staff and other departments. Everyone has a role to play in the identification of signs of concern. It is clear that people closest to the possible insider will detect changes sooner, but might also be more reluctant to report. Nevertheless, as it can be anyone in a facility, it is necessary that also everyone in the facility is aware of the threat and that signs of concern should be looked for.

In order to do this, you should have buy-in from management, as this is a sort of monitoring over personnel from everyone on everyone (also management). Evident partners, next to colleagues and the line managers, to have an idea on what is going on with a person are:

- Human Resources;
- Security staff;
- Medical staff (although there are clear restrictions in this area);
- …

To this regard, it also depends on who is working at the facility. In Belgium for instance, there are also many subcontractors who are working at the facility. Therefore, the relevant contact persons at the subcontractors' side also need to be identified, in order to gather and exchange information. It is important to define the specific partners in the organisation and to look in advance which information could be helpful and should be captured, depending on the situation. It is clear that not everyone can ask around about a person's private life, just because they are hesitating. It is important to have a reporting system, so the information is brought together and treated by someone who is identified and has the authority to do so, also to avoid the abuse of power of a superior over an employee. A colleague for instance, will not be in the possibility to check the records of Human Resources. If he reports this, the line manager can have certain information from Human Recourses and can bring the information together and maybe have a talk with the person in order to address the issue. Looking further up the chain, if the line manager reports someone after an analysis of the situation, he can provide the information to the security officer, who has more authority and for instance has the possibility to look into access logs and other collected data.

Looking at the further investigation and the analysis of the situation, external partners should also be identified. Certain information can for instance be checked with the security officer of the subcontractor, but also with local police forces, screening authorities or specific support organisations who have specific knowledge on a subject. A security officer cannot have knowledge on all possible topics, but, in Belgium for instance, he has the legal obligation to report. Partnerships with external partners to help interpret signs could be helpful. For instance, if there is an employee with signs of addiction, as this is a medical state, in many countries, such as Belgium, the security officer will not have the ability to ask for medical information. Nevertheless, if he has information on certain signs, he might be able to ask the external partners what the combination of these signs could mean (without identifying the person), in order to help the security officer react to the situation.

8. REACTION AND LEGAL RESTRICTIONS

Signs of concern that are reported must be handled. If nothing is done with the information, employees will not continue to report. Moreover, if a sign is reported before an insider act occurred and nothing was done with it, this could maybe have prevented the insider act from happening.

A reaction is therefore necessary, how to react is not easy to determine as in general it will need a case by case analysis. In general, the line manager or someone from Human Recourses seems the best person to react in first line, as (s)he can start by having a conversation with the person. It depends on the structure and the culture of the organisation who will be best equipped to do so. It is logical that a line manager will have a meeting with the employees once every while, so it does not raise the suspicion of 'being in trouble', when (s)he asks for such a meeting. This will generally also help the person who reported the sign, as it will be seen less as if (s)he has 'tattled on his/her colleague'. The line manager has a clear role in the reporting chain. Also, when a sign has been reported another way and was brought to the responsible person, the line manager is a key person in the decisions on how to react.

In Belgium, it will be the security officer who is responsible to handle the signs of concern. (S)He has the authority to do the aftercare and the legal possibility to conduct an investigation. In general, (s)he cannot do this alone, depending on the size of the organisation. The security officer should have a team in place with different expertise, in order to analyse the elements that have been reported, address the information that can be gathered and look at the actions to be taken. In order to analyse a situation it is necessary to have as much information as possible, as you are deciding on a person and his work.

In this regard, it is important to know what your legal possibilities are, these vary between countries, ex.: access to medical records, possibility for drug testing, possibility for access to HR records,… Moreover, as you are looking at privacy data, it is important to try and define in advance what information will and can be gathered and who will be in the possibility to look at the gathered data and the analyses. The culture of the country and the company will also define the analyses of reported elements. In some cultures, it is more expected that for instance, the line manager or someone from human recourses will have a conversation with an employee, in other cultures this act in itself can indicate that you have done something wrong.

In Europe the privacy laws have been strengthened by the General Data Protection Regulation. This regulation defines that privacy data can only be gathered for a specific defined reason and be looked at by those people who are in the necessity to see this data. Looking at reported signs of concerns, we are not in the possibility to define in advance which data will be gathered and which person will be needed to analyse the information. It is therefore useful that the security officer in this case has the overview and the authority to determine these aspects and that there are procedures in place in order to support his/her work and possibilities to gather information.

After the analysis, it is necessary to react to the elements that are known. As already mentioned, this is a case by case decision. Generally, at the end of an investigation, the person is decided to be a possible threat or not. When it is decided that there is no threat and no more actions will be taken, it seems useful to at least mention this to the person who reported the information. This will encourage the reporting system, as it is clear that information is being dealt with, nevertheless no more information should be given to this person, as we cannot reveal privacy data to a co-worker. When it is decided that the person is a possible threat or there is doubt, it is important to react in order to minimise the threat, this can be done for instance by:

- Asking the vetting authority for an additional investigation;
- Putting the person temporarily on a different function;
- Monitoring the person more closely;
- Firing the person;
- …

These possibilities could also be defined in advance. Nevertheless, these could be adapted depending on the situation. This is however a difficult balance, as you can cause damage by overreacting to the situation. By overreacting, you can break the trust with the employee, which could also strengthen his/her ideas and lead to an

insider action in itself. The reaction to a suspicious situation must be handled sensitively and proportionally to the known information.

9. CONCLUSION

The difficulty in this subject is that is impossible to have general guidance on the subject. The behavioural observation in an insider threat mitigation program is an aspect that is being looked at in every country, but as it depends on the legal possibilities and on the culture as well as the specific situation that is being analysed, you cannot put this into one guidance. Moreover, as it is a sensitive subject and it often contains personal data, concrete cases cannot be shared in all details.

Reporting and reacting to changes in behaviour is a difficult balance: if you overreact, the person could become an insider; if you underreact, an insider act could happen. Therefore, it is important to have a mechanism in place so every sign can be addressed and be analysed properly before deciding if and how to react to it. It is a good practice to discuss these individual cases in a multidisciplinary team, in order to bring all elements together. The basis for the mechanism is that everyone is aware they should look out for signs of changing in behaviour and that they could report it.

In the analysis and the reaction, we need to have an overview of the legal possibilities on what to gather and how you could react. The reaction in itself is a difficult balance between protecting the rights of the individual and protecting the facility. This is not a ‘one size fits all’ solution, as again, this depends on the legal framework and on the culture in the country and the facility.

It is therefore important to share experiences from all over the world, and have an overview of some best practices we can learn from and that can be modified to your own situation.