ON SCREENING AND THE INSIDER THREAT – A METHODOLOGICAL EXPLORATION

Dr. Giliam de Valk[1]

ABTRACT

An under researched issue in security is screening combined with the insider threat. One of the problems is the lack of data. Human Resource Management (HRM) departments don’t like to disclose cases and modus operandi. Also the filing is incomplete. It leads to a situation in which theory building is hardly possible. Therefore, this explorative essay is written from a more methodological perspective.

From the scarce information that was obtained from expert practitioners, there seems not to be such a thing as a standard profile of an insider threat. At the same time, an estimated 75% of the offenders has shown to have been actually bona fide at the original pre-employment screening. It calls for a reflection on current screening practices.

[1] In 2005, Giliam de Valk published his PhD on the quality intelligence analyses have to meet. He is specialized in the methodology of security and intelligence analysis. He has worked at the University of Amsterdam, the University of Utrecht, and the Netherlands Defense Academy where he coordinated and lectured a minor on intelligence studies. At the moment he is an assistant professor at the Institute for Security and Global Affairs, Leiden University.

Such an approach has its limitations. Scenarios for offenders cannot be built, because the causes are too diverse and the cases too unique. As files are hardly kept – and HRM departments are not so willing to share – a big data approach is also not a likely option.

A way out could be to test the loyalty of employees. In such a system, the emphasis will be on a so-called during-employment screening. The interviewer, together with the applicant, will assess the applicant's vulnerabilities. After this assessment, the applicant will be tested on his/her vulnerabilities during his/her entire career,

Also, there needs to be a shift in the culture at HRM departments. They have to change from steering on mistakes, into being a safety net for employees that have (personal) problems. It also implies a change in interaction – from discussion to dialogue.

Finally, in a working environment that is evolving towards a more networked way of working – compared to the classic hierarchical office work – the rethinking concerning the screening practices will only be the more pressing.

Keywords: critical infrastructure, insider threat, HRM, screening, in-employment, during-employment

1. Introduction

At the Ad de Jonge Centre of the University of Amsterdam,[2] an experiment took place that triggered a reflection on the current screening approach. At this experiment, it was looked for so-called weak signals – small patterns that are difficult to detect in the midst of an overwhelming noise of data, events and developments (Hard Rudman Commission, 2008). It resulted, among others, in a weak signal that could be a game

[2] In 2017, the Ad de Jonge Centre moved to Leiden University and integrated in the Institute for Security and Global Affairs. It transformed into the intelligence working group of the ISGA.

changer on the middle and long term. It was on a possible trend in mindset within the Western world.

This weak signal was found in psychological surveys. Nowadays, students in the Western world are said to be 40% less empathic, and to suffer from an increase in Narcissism (Twenge, 2008a. Twenge 2008b). They tend to be more egoist, competitive, self-assured, individualistic. And it was claimed that there is a correlation with utilitarian responses to moral dilemmas (Bartels & Pizarro, 2011. Dutton, 2012). Such research findings are debated, but it served as a trigger to question if the current screening approach would be adequate for that possible change in mindset.

Another element also triggered the reflection on the current screening practices at the critical infrastructure. This is the change from the traditional professional bureaucracy – with its classic hierarchical office-bound way of working – to a more networked based organization in which people also work from home. The new environment asks for more agility within organizations. Organizations are likely to move from a top down controlled and economic goal driven structure into a more viable system of self-organized and -managed structures. There will then be more emphasis on being unique resources centered and human value driven – organized around social values and goals, social legitimacy and commonality. It may lead to a shift in the way Human Resource Management (HRM) will function – from the concept of 'best principles' as a strategy, into one of recommended practices (Houtzager, 2018. Boselie, 2010).

A problem with studying screening policies and the insider threat in the context of critical infrastructure is that data is rarely disclosed publicly. It was not, for example, a focal point in the reports by the National Advisory Centre Critical Infrastructure (NAVI).[3] Also more generally, HRM departments are not very keen to display their data on insider threat offenders, or their modus operandi. Theory building is almost completely lacking. Therefore, this article is an

[3] The NAVI - Nationaal Adviescentrum Vitale Infrastructuur - ceased to function in 2010, after it has made its assessments on the different vital infrastructures in the Netherlands. Advisors of the NAVI continued its activities in the Adviescentrum Bescherming Vitale Infrastructuur. http://www.adviescentrumbvi.nl/search_stats_over_ons.htm, consulted May 2018.

exploratory essay in this field. It reflects on the current screening practices without having an elaborate set of data or theory building. The findings will therefore be only preliminary findings. As an academic exercise, this is risky. The author realizes this. Yet, the interests at stake in the critical infrastructure are too high to leave this field undebated.

2. Types of screening, and risks and threats

There are different forms of screening. In this section, they will be defined in the sense they are discussed in this article (2.1). Furthermore, I will reflect on how different ways of screening are rooted in different methodological backgrounds (2.2).

2.1 Types of screening

Screening: to investigate systematically if the information given by the candidate/employee is in accordance with reality, and if no relevant information is being withheld (VBN, 2018).

Pre-employment screening: to carry out a positive vetting of a potential candidate (VBN, 2018). Data and information are collected to assess the risks in order to see if a tenure is justified.

In-employment screening: periodically carrying out a screening for those employees who get a new function or responsibility within the organization where they are working (VBN, 2018). This often happens if they get more competences or responsibilities. In the Dutch practice, this is often a shortened version of the pre-employment screening.

Post-employment screening: A screening and exit briefing when an employee leaves the organization (VBN, 2018).

During-employment screening: a combination of a pre-employment screening – in which the vulnerabilities of a candidate are assessed – and of tests on his/her vulnerabilities during the entire employment, to refute that this person poses a threat.

2.2. Screening: risk mitigation or threat approach?

A *risk* is the chance that an incident might take place, multiplied by the impact: the quantitative multiplication of the probability of the occurrence of an event by its estimated impact. In risk mitigation, you try to reduce the number of incidents and the impact itself (compare: Glendon, 2016) The focus is on *assessing* the risk.

A threat is here shortly defined as an undesirable event that you do not want to take place. A threat does not necessarily cause actual harm. It is on the nature of occurrence (National Information Assurance Training and Education Center, consulted in 2013). In a threat approach, you do not want that the event takes place in the first place.

Most of the types of screening are based upon risk mitigation. In the Dutch context, both the *pre-employment* and the *in-employment* screening are meant *to assess the risks* of the candidate/employee in order to see if a tenure/promotion is justified. In the *during-employment* screening, on the contrary, the tests on the person's vulnerabilities are meant to *refute* that an employee poses a *threat*.

This difference in risk and threat approach is fundamental, and refers to the α and the β. The α is the chance that you incorrectly conclude that there is a significant relationship between phenomena. The β is the chance that you do not discover a weak, but actually existing, relationship between phenomena (De Valk, 2005, 66-67). In the *pre-employment* screening, the emphasis will be on reducing the value of the α – the chance that HRM incorrectly assesses the risks of the candidate. In the *during-employment* screening, the emphasis will be not missing a threat – to reduce the value of the β. We will return on the α and β, in the evaluation of preferred ways of screening.

3. The Dutch context

In the Netherlands, there is not much available data on screening. If there is data, it is, for example, on people who did not pass the pre-employment screening and subsequently were rejected for the job (Levent Bedrijfsrecherche, 2018 in: VBN, 2018). But this is not the same as the correctness of those rejections. It also gives no insight in the number of people who actually passed the pre-employment screening and then, after the screening, turned into an insider threat. In methodological terms, the data on people who passed the screening does not tell anything about the Type I and Type II errors of this pre-employment screening process. What is the number of the people that were incorrectly rejected from getting the job (Type I error)? And what is the number of the people that passed the screening, but where actually a threat that was missed (Type II error)? In short, this data gives no insight in the validity and accuracy of the pre-employment screening process.

Information on screening and the insider threat is scarce. It is even more scarce in surveys. One of the few exceptions is a publication by Sollie and De Weger in which it is hinted at the need of more in-employment screening, especially in relation to military missions (Sollie & De Weger, 2011). Yet, the focus in this research is on crossing to the dark side, and not on the type of screening. The main problem for this lack of data is obvious – HRM officials are not too happy to disclose their failures.

Still, some data is present. However, it concerns unpublished research findings – with a request of no referencing. The following results were found. The first set of findings was that four elements appeared more than average in offender cases:

1. Employees with open-ended contracts were more often offenders than their colleagues with fixed contracts.

2. Employees working more than 10 years at the same organization were overrepresented as offenders.

3. More than average, a life changing event had taken place.

4. Employees with a Narcistic personality were overrepresented.

Still, these four elements did not result in a typical profile, even not in combination. For that, the correlation was simply too low, and the number of variables too big. The causes were too diverse and the cases too unique.

A second set of findings concerned the relationship between the original pre-employment screening and the actual derailing of the employee. After a reconstructions of the cases, the remarkable number of an estimated 75% of the employees showed to have been actually bona fide at the original pre-employment screening. This last finding puts a serious question mark at the current practice of *pre-employment* screening. If this data is correct, it implies that the current system of *pre-employment* screening will miss 75% of the cases of people that later will derail. Is there a serious Type II error in our current *pre-employment* screening practice?

4. Analytical methods and techniques

If we indeed miss so many cases, we need to reflect on the current method of screening. Furthermore, changes may be needed in how HRM departments function. In this section, we deal with the method and will look, from a methodological perspective, at alternative options. In the next session, I will discuss the HRM.

Firstly, we need a warning system for the insider threat, For that, we can look at an established warning system for inspiration. In the military, there is the NIWS – the NATO Intelligence Warning System (NATO, 2001. See also: Grabo, 2002). It is based upon warning scenarios. For each warning scenario, a limited number of so-called critical indicators are developed. 'Critical' refers to a given scenario that will take place if its indicators move into red – the warning mode. To use this for the insider threat, however, will cause problems concerning the formulation of the warning scenarios. In case of the insider threat, the causes are too divers and the cases too unique. NIWS often works with three scenarios. Working out an endless number of scenarios is not only not workable, you still may miss relevant scenarios due to the uniqueness of the cases.

There is also a policy oriented version of scenario building. Often drivers on actors and factors are analyzed, and from there on, scenarios are constructed.[4] But also here occurs exactly the same problem – an endless number of scenarios for unique cases, that still will not cover the whole picture.

A third option could be big data analysis. The main problem is the data. As put, HRM departments are not very keen to display their failures or data. As we will discuss in the next session, there is even a problem at the input side of data – the practice of not reporting. The lack of data, combined with the diversity of causes and unique cases makes a big data analysis also an unlikely option.

If we would choose one of the above options and construct some scenarios or flawed big data analysis, it would lead to too many Type I and Type II errors. Type I errors could be triggered by simplistic scenarios – caused by the absence of

[4] This way drivers are assessed at the course Qualitative Analysis Techniques. This course is part of the Minor Intelligence Studies at the Institute for Security and Global Affairs, Leiden University.

data and the diversity of causes – and would stigmatize whole groups of employees, as those being more on the Narcistic side of the spectrum. Anyone in the intelligence community who is familiar with misdirected mole hunts, knows how damaging these are. A high number of Type I errors would trigger a tsunami of misdirected mole hunts. So, the methods mentioned are not an option to cope with the insider threat.

What remains as an option is what is called in methodology the experiment. In this experiment, the loyalty of the employee is tested. Such tests need to be prepared well. It requires an extended interview with the candidate/employee, but of a different nature than in the current pre-employment screening. The experiment is organized around the principle that the employee does not pose a threat. It is a threat approach, contrary to the pre-employment screening which is primarily a risk approach. The experiment is aimed at to lower the value of the β. Such an experiment to lower the value of the β is also called a red team test (De Valk, 2018). We will return to the option of the experiment, after dealing with the HRM.

5. HRM

As put, HRM is not very keen to share their failures, or data on offenders. As a result, other HRM departments cannot learn from incidents. Also within the own organization, its employees don't know where to look for.

This last point is combined with an even more worrying observation – and that is the common culture at HRM departments. Often, the HRM acts on mistakes of employees, but it is not a safety net for employees that have (personal) problems. The effect is that the person in question, in case he/she is vulnerable (e.g. after a life changing event), will not contact HRM for help. Also his/her colleagues will hardly have incentives to report on suspect indicators and behavior. The same applies to the superiors of the employee in question. Superiors hardly tend to keep files. Both in the case of the colleagues and the superior, it explains the low willingness to report to the HRM. It results in a too little & too late situation, at least for the Dutch situation. At the same time, it is for insiders often not a surprise that things went wrong – the indicators were there. This implies the need for a different culture within HRM departments (Houtzager, 2018).

According to Houtzager, an important aspect of prevention is to move from discussion to dialogue. The focus is then solely asking questions to the other person. This way you support the other person in explaining his/her point of view and it helps to understand the person better. For that, the person who asks the question, also needs to ask him/herself questions – to start a dialogue with yourself. There is a mutual interest in each other by asking questions. That opens the way to a real dialogue (Houtzager, 2018). This is an attitude that differs very much from the common practice of HRM departments to steer on mistakes.

To what recommended practice of screening may that lead the methodological insights and insights on the culture at the HRM?

6. How to organize the screening against the insider threat?

This section starts with two ideal types of screening. The first ideal type is on risk mitigation (pre-employment screening), and the second one is on threat assessment (during-employment screening). The two forms as presented here are not the actual ones used in practice, which are to a certain extent mixtures of both. But by presenting them as ideal types, the working between both types can be explained more clearly. Both ideal types of screening were for many years part of an assignment for students of the Minor Intelligence Studies – first at the Ad de Jonge Centre (University of Amsterdam), and later at ISGA (University of Leiden) – to train them in Type I (α) and Type II (β) errors.

6.1 Two ideal types of screening

An ideal type does not refer to an ideal or desired situation. It refers to a ‘pure’ version, in order to explain and show its working.

The first ideal type is on the *pre-employment screening*. In this ideal type, it is *assessed* that the candidate does not pose a *risk*, and does not live in a vulnerable environment. To carry out this screening an elaborate background check is made. The interview with the candidate is organized as follows:

- an extended interview of 4-6 hours is held. This is carried out by two persons, of whom one is the interviewer and the other the observer.

- the aim of the interview is to assess whether the candidate is vulnerable (e.g. alcohol, drugs, sex, money, past, etc.), or has an extremist/violent past. The emphasis is on the candidate's life from 16 years old onwards.
- the aim is also to assess whether there are any vulnerabilities in the environment of the person, like extremists, criminals, or visiting pariah states.

The second ideal type is the *during-employment screening*. During his/her entire career, the employee can be tested on his/her vulnerabilities. To do so, an elaborate background check was made, as in the case of the previous pre-employment screening. The major difference is in the interview and the follow-up process. This is a three phased strategy in order *to falsify* that the person poses a *threat*:

- phase 1 is composed of a long interview, even up to more than 10 hours. The interview is held by one person in order to build up rapport. The interviewer asks the candidate to describe him/herself now, and from there they go back in time. Finally until the candidate was 3-7 years old. This will also give insight in some more primary and fundamental patterns that are less investigated in the first ideal type.
- in phase 2 the vulnerabilities of the candidate are assessed. Together – interviewer and candidate – they make a plan of how to cope with these vulnerabilities.
- phase 3 encompasses the entire career of the employee. He/she can be tested – red teamed – during his/her entire career on his/her vulnerabilities, in order to *falsify* that he/she poses a threat.

6.2 Methodological advantages

The two ideal types are based upon two different methodological approaches. The *pre-employment screening*, as it is described here, is a *risk assessment*. It is primarily related to reducing the value of the α. It is about *assessing* that the candidate does not pose a *risk*. The risk assessment approach is dominant in the guidelines of the VBN.

The second ideal type of *during-employment screening* is about *falsifying* – to refute – that the candidate poses a *threat*. It is a *threat assessment* that is aimed at *not missing* a threat. It is primarily related to reducing the value of the β.

If we look at both methodological principles, which is the more reliable one: to assess/proof someone's integrity and loyalty, or to falsify that someone poses a threat? From a methodological perspective, to try to *falsify* – to refute – is the more reliable approach and therefore the standard in, for example, scientific hypothesis testing (De Groot, 1981). From a pure methodological perspective, it means that the second ideal type – that of *during-employment screening* – is the preferable one.

But also if we look at the actual data on pre-employment screening, the remarkable number of an estimated 75% of the insider threats showed to have been actually bona fide at the original pre-employment screening. It implies a huge number of Type II errors, in which the current system of pre-employment screening misses 75% of the cases of people that later will derail. The practice of pre-employment screening has a very serious problem with the value of the β. At the same time, no (published) data could be found on the value of the α – of candidates that were unjustly or unnecessarily were rejected. We will come back on that in the next session 6.3.

6.3 Other advantages

Besides that during-employment screening has the stronger methodological approach than pre-employment screening, it has some other additional advantages. Firstly, as it is the stronger form, there is a lesser change on unjustly rejecting a candidate – that is still a dark number in the current practice of screening. In case of doubt – e.g. of a 'vulnerable subcultural' environment (as the sailor experienced in the more wild side of life) – the candidate does not need to be rejected, but can be tested on that vulnerability.

Secondly, you can avoid a monoculture within your organization. As it is assumed that everyone has vulnerabilities – and this will be tested during their career – you can diversify more among the population, subcultures, and minorities. Now, there is – at least at the Dutch services – an overrepresentation of employees with an autochthonous (higher) middle class background, who have had an academic education and grew up in a rather protected environment (the pre-employment screening, by definition, favors candidates from a protected environment – as this is an explicit part of the assessment). A former employee of the AIVD characterized it as an overrepresentation of liberal women who – before work – bring their offspring to school in their carrier tricycle for children (Versteegh/*NRC* 2018). Although this quote was criticized for its implicit sexism, it points at major problem – the danger of a monoculture that will lead to a blind spot. To deal with the blind spot, you need different perspectives within your organization (compare Zizek, 2006).

Thirdly, if a case is brought to court, the during-employment approach is the better option for the employer. The employer does not have to hand over elaborate files with evidence to proof the case – and by that have a lot of exposure. The employer simply can state that the employee did not pass the red team test.

Fourthly, by going back in time further – 3-7 years old – it can be better assessed how someone will function under pressure and what the primary patterns are.

Fifthly, going back in time – from the present to the past – will give less room for deception. This is a classic interrogation technique.

Sixthly, an interview by one well-trained and experienced person gives more opportunity to build up rapport and avoids resembling an interrogation-style interview. Building rapport is also known as an effective interrogation technique to get more information out of a suspect (Dimitriu, 2009).

The ideal type of *during-employment screening* is not only the stronger methodological approach, it also has some extra advantages that the ideal type of *pre-employment screening* does not have.

6.4 HRM

The measures should not be limited to the way the screening is carried out. The culture at the HRM should change in the first place. HRM should abandon its common approach of steering on mistakes. HRM should change it into being a safety net for people that have (personal) problems. Only then, these employees will ask for help, their colleagues will report on indicators, and their superiors will be more willing to keep files. The whole attitude within the organization should change from discussion to dialogue.

7. Conclusion

This essay started with two observations on changes in society – the possible changes in mindset and the differences at the working environment. They formed the triggers to reflect on the current Dutch screening practices. The findings of this essay are based on methodological insights, literature on HRM, and scarce and unconfirmed data. Therefore, only preliminary conclusions can be drawn. All the evidence, however, pointed into one direction concerning two issues. These two preliminary conclusions will be presented here.

Firstly, the culture at companies, and especially at the HRM, needs to change. From steering on mistakes, into being a safety net for people that have (personal) problems. It also implies a change from discussion to dialogue. This will increase the grip on the insider threat issue.

Secondly, the current pre-employment screening practice needs to be revised. In open sources, we can find data on how many people were rejected for a job. But it doesn't tell anything about the Type I and Type II failures of that type of screening. Unpublished research findings suggest that 75% of the employees were shown to have been actually bona fide at the original pre-employment screening. With such a high number of later derailment, you may wonder if the pre-employment screening is the right approach at all. The value of the β is too high.

There are alternatives. In *during-employment screening* an employee will be tested on his/her vulnerabilities during the entire employment. This approach is not on assessing a risk – as in pre-employment screening – but on *falsifying a threat*. From a methodological perspective, refutation is the more reliable approach. Also, if screening results are put to the test in a trial, the employer simply can state that the employee did not pass the red team test, instead of handing over elaborate proof that the employer would rather have had kept undisclosed.

It is not advocated to apply the during-employment screening for all cases. A distinction could be made between functions that only will result in risks with a limited potential damage, and those where the organization's future or national security might be at stake. If there is only a limited risk, you just want to minimize the number of incidents and the level of damage of those incidents. A risk approach – as in pre-employment screening – could then be accurate. But all cases that would lead to a threat of the organization or national security – the real sensitive functions – a threat approach seems more suited. In that case, during-employment screening with its approach of falsifying that the employee poses a threat seems to be the appropriate one. Such sensitive functions and positions within the critical infrastructure need an improved protection. In short, a threat approach is needed if the national interest is directly at stake.

During-employment screening is not completely unknown in the Dutch context. But as a central focus in a HRM policy, it is new. It requires that guidelines are updated, as the one by the VBN. In that guideline, meant to last until 2023, the emphasis is on risk management. The threat approach and the culture at HRM's are almost completely absent. An update is needed, and one may wonder if the Dutch society has the luxury to wait until 2023 before doing so.

References

1. Adviescentrum Bescherming Vitale Infrastructuur. http://www.adviescentrumbvi.nl/search_stats_over_ons.htm, consulted May 2018.
2. Bartels, Daniel M. & Pizarro David. A. (2011), The mismeasure of morals: antisocial personality traits predict utilitarian to moral responses, *Cognition*, (2011, 154-161).
3. Boselie, Paul (2010), *Strategic Human Resource Management - A balanced approach*. Mcgraw-Hill Education, 2nd print.
4. Dimitriu, George (2009), Ongeoorloofde pressiemiddelen tijdens ondervraging in extreme situaties, *Militaire Spectator*, number 5, 2009, 274-290.
5. Dutton, Kevin (2012), *De lessen van de psychopaat*, Amsterdam: De Bezige Bij.
6. Glendon A.I., Clarke, S. McKenna, E. (2016), *Human Safety and Risk Management*, CRC Press, second edition.

7. Grabo, C.M. (2002), *Anticipating Surprise: Analysis for Strategic Warning*. Washington: DIA.
8. Groot, de (1981), *Methodologie. Grondslagen van onderzoek en denken in de gedragswetenschappen*. Den Haag: Mouton, 1981 (11th print).
9. Hard Rudman Commission (1999), *New World Coming: American Security in the 21st Century Study*. Addendum.
10. Houtzager, Wil (2018), *Insider Threat. How organizational culture influences the insider threat*. Lecture at University of Leiden, 11 October 2018
11. National Information Assurance Training and Education Center (consulted in 2013), *Glossary of Terms*, http://niatec.info/Glossary.aspx?/term=5652&&alpha=T
12. NATO (2001), *Generic Early Warning Handbook*, EAPC(COEC)D(2001)2.
13. Sollie, Henk & De Weger, Michiel (2011), *Crossing to the dark side Een verkenning naar extremisme en terrorisme vanuit krijgsmacht en politie*, Breda: NLDA.
14. Twenge, Jean. M., a.o. (2008), Egos inflating over time: A cross-temporal meta-analysis of the Narcissistic Personality Inventory. *Journal of Personality, 76*, (2008, 875-901).
15. Twenge, Jean M. a.o. (2008), Further evidence of an increase in Narcissism among college students, *Journal of Personality*, (2008, 919-927).
16. Valk, G.G. de (2005), *Dutch intelligence - towards a qualitative framework for analysis: with case studies on the Shipping Research Bureau and the National Security Service (BVD),* Boom Juridisch*.*
17. Valk, G.G. de (2018), Critical Infrastructure and The Unknown: A Methodological Quest, *National Security and the Future*, 2018: 19(1-2): 15-44.
18. VBN/Vereniging Beveiligingsprofessionals Nederland (2018), *Nationale Richtlijn Pre-, In- en Post-Employment Screening. Versie 3.0, 2018-2033*.
19. Versteegh, Kees (2018), De politiek krijgt te veel invloed op de AIVD in: *NRC Handelsblad,* 15 February 2018.
20. Zizek, S. (2006), *'The Parallax View. The Stellar Parallax: The Traps of Ontological Difference'*

http://www.lacan.com/zizparallax.htm (consulted in 2018),