Reporting Security Concerns in the Nuclear/Radiological Industry: New Evidence to the Study of Whistle-blowing

Iryna Iarema and Katherine M. Bachner

Nonproliferation and National Security Department, Brookhaven National Laboratory, Upton, NY, 11973, Office: (631) 344-8271
E-mail: iryna.iarema@hotmail.com, kbachner@bnl.gov

Abstract:

The international community stresses the necessity to report discrepancies in security procedures and build an environment conducive for fostering security culture inside organizations that handle nuclear or radiological materials. In reality, however, there have been a number of instances where reports on nuclear security were not encouraged by organizations or were left without needed corrective actions. Such an attitude, where reports on security matters, instead of serving as an internal 'early warning signal' leading to enhancement of security, have been put aside or entered the public domain after external reporting, is to a great extent caused by a lack of knowledge on how to deal with them and what drives people to report.

This article aims to study challenges and drivers for reporting in the nuclear and radiological sector. First, it discusses the meaning of whistle-blowing and reporting. Secondly, it demonstrates how reporting is encouraged by the international community through IAEA guidance and Nuclear Industry Summit statements. Then by using survey data received from 56 participants, the study examines factors influencing reporting. This analysis is supported by an overview of some real-life examples related to reporting or raising concerns about security procedures in organizations that handle nuclear or radiological materials.

Keywords: whistle-blowing; reporting in organizations; nuclear security; nuclear security culture; drivers of reporting

1. Introduction

With an anticipated expansion of low-carbon energy derived from nuclear technologies or the so-called 'nuclear renaissance' [1], measures should be taken to ensure their safe and secure operation. The role of whistle-blowing is salient in the context of dealing with an insider threat, especially when, as Glynn and Bunn [2] assert, '*nearly all of the documented thefts of highly enriched uranium (HEU) or separated plutonium* […] *appear to have been perpetrated by insiders*'. This problem is becoming especially acute in the light of amplification of terrorism networks and the risk of their infiltration into organizations that handle nuclear or radiological materials. In such a situation, an employee of a nuclear (or radiological) organization is in the best position to observe a deviance in nuclear security or suspicious behavior and report about it. In addition to that, reliance on reporting could play a pivotal role in deterring and preventing wrongdoing in organizations that handle nuclear or radiological materials.

Being largely instigated by the fact that reporting in the nuclear security field has not yet received a broad discussion in the academic literature, this study will contribute to filling this gap. It hopes to unveil factors that may lead to a greater understanding of the impediments/inducements for the operationalization of whistle-blowing in the nuclear/radiological sector. For example, in relation to nuclear **safety** culture, the IAEA recognised the value of reporting to help continually improve organizational practices and encourages maintaining '*a "blame-free" reporting culture*' to spur '*full reporting of unsafe or unethical practices, incidents and near misses*' [3]. Similarly, increased knowledge about factors influencing reporting of **security** concerns will help to channel management in nuclear organizations in the correct way, bringing practical benefits resulting in better protection of sensitive nuclear materials and facilities.

1.1 Definitions

Although defining whistle-blowing is challenging, there is a need to be explicit about what exactly is meant by the terms we utilize in the current study. Perhaps, the most commonly used definition of whistle-blowing was first provided by Near and Miceli in 1985 [4], according to which whistle-blowing is '*the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action*'. Some [like C. Peters and T. Branch referred in 5] pointed to whistle-blowing as '*the act of disclosing any information that an employee reasonably believes evidences a violation of any law, rule or regulation, mismanagement, corruption, abuse of authority, or threat to public health and safety at the worksite*'. Jubb [6] identified six elements that might be subsumed under the term whistle-blowing: '*act of disclosure, actor, disclosure subject, target, disclosure recipient, and outcome*'.

Interestingly, regulatory provisions in the chemical industry – namely, the U.S. CFATS Act of 2014 [cited in 7] speaks

Iarema, I., & Bachner, K.M. (2018). Reporting Security Concerns in the Nuclear/Radiological Industry: New Evidence to the Study of Whistle-blowing. *ESARDA Bulletin - The International Journal of Nuclear Safeguards and Non-proliferation*, 57, 2-21. https://doi.org/10.3011/ ESARDA.IJNSNP.2018.7

about facilitation of whistle-blower reporting as '***reports** of potential CFATS violations* ***from employees and contractors*** *at chemical facilities*', thus expanding the scope of reporting to a broader circle of actors. Building upon this, we would use term *whistle-blowing* with regard to the to the acts of disclosure carried out by an employee or former employee ('*whistle-blower may leave the organization before blowing the whistle*' [4]) or a current or former contractor who reports *internally or externally* about wrongdoing (or lack of actions when they are warranted) in the nuclear or radiological field. Throughout this study, we will also refer to terms such as *reporting* or *informing* and use them interchangeably with *whistle-blowing* to avoid repetition.

2. How reporting of breaches in nuclear security is regarded in international statements

Attention to the issues of reporting security concerns in the nuclear and radiological field is relatively young, nevertheless not without important international commitments, though non-binding. The most prominent in addressing issues of reporting have been: Nuclear Industry Summits and International Atomic Energy Agency (IAEA) guidelines and recommendations.

Started in 2010, Nuclear Industry Summits highlighted the importance of reporting procedures and vigilance for nuclear security matters. In particular, the appeal to '*fostering an open environment for reporting security concerns*' was made in the Joint Statement of the 2012 Seoul Nuclear Industry Summit [8]. In addition to this, the Joint Statement of the 2016 Washington Nuclear Industry Summit [9] also called for '*encouraging employees to report suspicious behavior and/or events through appropriate channels*' [9].

The International Atomic Energy Agency recognizes that the scope of nuclear security extends to '*nuclear and other radioactive material, associated facilities and activities*' [10]. On the level of implementing guides, the IAEA emphasizes the importance of reporting processes for fostering nuclear security culture by such statements as:

> *'Managers need to encourage personnel to report any event that could affect nuclear security. This entails encouraging personnel to provide the security staff with information that could affect security, rather than keeping the information to themselves'* [11].
>
> *'For security, there is the particular need to ensure that staff members understand that adherence to the policy is expected of all personnel. These expectations include protecting information, being aware of potential security concerns and threats, and being vigilant in reporting security incidents'* [11].

The IAEA includes presence of reporting mechanisms to the indicators of a strong nuclear security culture [11]. This international body sees '*protection of individuals who provide information for the purpose of protecting the integrity of nuclear security*' as an antecedent to the establishment of a nuclear power program [12]. Thus a state considering the construction of a nuclear power plant should develop a legislative and regulatory program that contains necessary provisions governing such aspects as whistle-blowing as part of its nuclear security infrastructure [12].

The IAEA model of nuclear security culture has 30 culture characteristics, some of which relate directly to whistle blowing or reporting. For example, to establish and facilitate the process, the model includes characteristics such as a feedback process in management systems, involvement of staff and effective communications in leadership behavior and vigilance in personnel behavior. Culture indicators associated with such characteristics are designed to set standards as well as to provide appropriate tools for periodic implementation of self-assessment, with the focus on whistle blowing and reporting.

Despite the importance of the statements made at Nuclear Industry Summits and recognition of the value of reporting by the IAEA, the process of reporting has not yet been exploited to the full for its capacity to strengthen security inside organizations that handle nuclear or radiological materials. Difficulties arise with practical implementation. Here, Bunn [13] rightfully admits '*Convincing people to report incidents in which they or their colleagues made mistakes or broke the rules is not easy. But experience demonstrates that with the right approach, a culture of reporting can be forged within an organization*'. This begs the question: what is the right approach for encouraging reporting in organizations, and can it be done without deteriorating staff morale? Referring to Miceli et. al. [14], we agree that there are ethical ways to stop wrongdoing via reporting, and information about something which might inflict harm to a large number of people, an organization, the environment, etc. should not be concealed.

Since step-by-step practical guidelines and detailed recommendations are lacking for establishing reporting mechanisms in nuclear and radiological fields, we suggest studying the current state of affairs and the attitudes of professionals toward reporting. In addition to the empirical data gathered by us, this study will also include analysis of the merits of real-life situations on whistle-blowing disclosed in the media or academic literature. A detailed description of our main methodology follows in the next section.

3. Methodology and data

3.1 Description of the methodology

We conducted a survey among people working in the nuclear or radiological industry. The purpose of the survey – to study drivers and challenges for reporting security breaches and actions potentially leading to security breaches within organizations that handle nuclear or radiological materials – was mentioned in the cover letter of an e-mail invitation and its on-line description. The survey consisted of 16 questions and required a total of 10 minutes on average to complete. Questions were formulated in both English and Russian. The survey was available online at the popular on-line cloud-based survey software service for filling out from October, 27, 2016 until November, 7, 2016.

Despite the somewhat sensitive topic, we took several steps to ensure we received enough responses for making this analysis. First of all, the survey was anonymous; the respondents were required only to provide some demographic data. Invitations to fill in the survey were sent to people who work in organizations that deal with nuclear or radiological materials; they were among the professional contacts of the authors or participants at thematic events. The invitation also included a dissemination request. The information about the survey was published on the webpage of the World Institute for Nuclear Security.

As a result, we received 56 completed surveys, which is sufficient, in our view, to make some generalizations on the subject. It is also important to mention that some of the respondents skipped some of the questions, although we suspect that in most cases it happened rather because of an accidental omission than due to purposeful omission. A more detailed account of the profile of our respondents follows.

3.2 Data about survey respondents

3.2.1 Organizational data

Subjects of the study were people working in the nuclear or radiological field (only one person declared that he/she does not work in such a field) who voluntarily participated. They represented different professional roles, which is beneficial for gaining a diverse perspective on whistleblowing in the field. Professional roles were almost equally split (each around 20%) among security specialists, researchers, managers and other categories, a description of which is provided in Figure **1** below.

The majority of our respondents (85.7%) indicated that they have more than 5 years of experience in the nuclear or radiological industry, among whom those who worked in the industry more than 10 years constituted 62.5%. Those who have worked from two to five years in organizations that deal with nuclear or radiological materials comprised 10.7% (see Figure **2**).

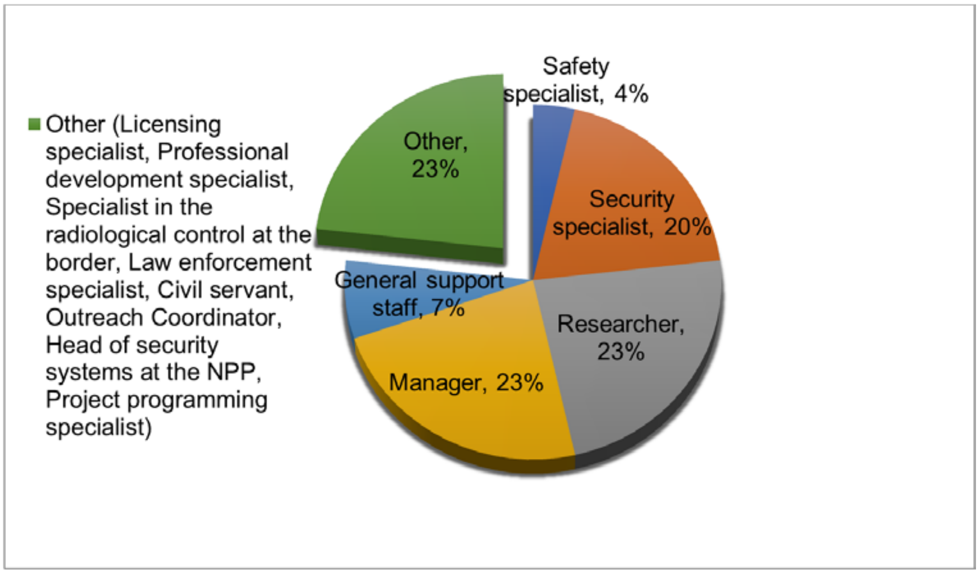

Figure 1: Professional roles of the respondents

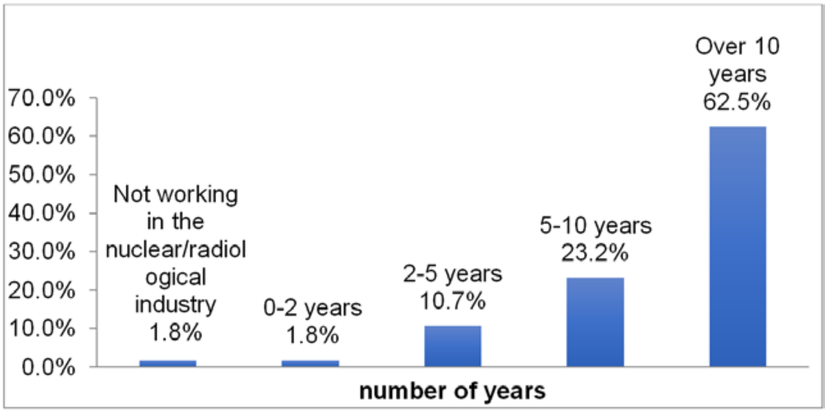

Figure 2: Number of years of experience (of respondents) in nuclear or radiological field

Some studies have indicated that organizational tenure can influence the likelihood of whistle-blowing [15]. Reportedly, newer employees with less experience are less likely to report wrongdoing than more senior fellows, partly because of not being aware of the operational climate in the organization [Dworkin & Baucus, 1998 referred in 15] or appropriate channels for whistle-blowing [Miceli & Near, 1992 referred in 15]. One might see some potential benefits in building upon the argument of organizational tenure to see how to assure a climate favorable for raising valid concerns among less experienced employees and contribute to their empowerment for following organizational procedures of security. For this, one would need to conduct a research study with a larger sample, with follow-up focus groups to develop a reliable picture for the nuclear/radiological industry.

Out of 56 respondents who completed the survey, half work in Ukraine (see Figure **3**). Approximately 29% work in the USA, 5.4% in the U.K. and the rest (approximately 16%) in such countries as Austria, Canada, Germany, Italy, Lebanon, Lithuania, Moldova, and Serbia.

Some studies carried out by Ernst and Young indicated that even in Europe in multinational companies, respondents in the United Kingdom differ from those in France or Austria with regard to their willingness to blow the whistle, where the former would feel more comfortable than the latter [14]. The intention to blow the whistle could also be influenced by regulatory provisions, which in the USA and UK are reportedly more clearly defined than in other countries [14]. In the UK, for instance, the law ‘*denies protection to whistle-blowers who give information for gain*’, whereas in the USA there is, reportedly, no prohibition against a reward for whistle-blowers [14]. Despite some differences, there are also similarities among countries like the USA and UK, including cultural [14], which also draws our attention to the prospects of exploring cultural phenomena and their influence on reporting mechanisms. This is especially important since in some environments, due to interpersonal tensions, whistle-blowing may be used as a tool to avenge personal grievances or injuries outside the security area.

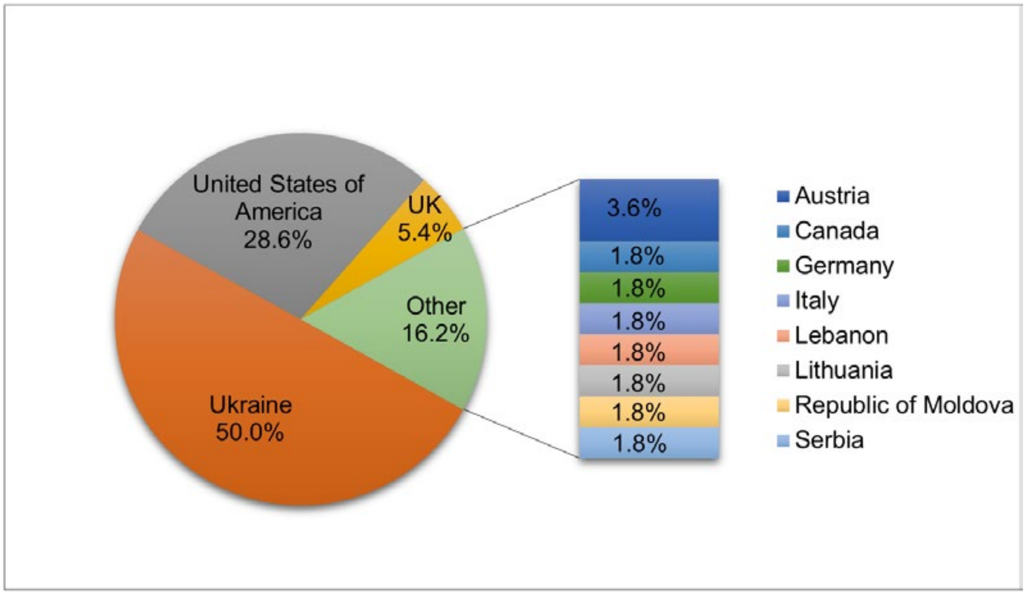

Figure 3: Countries, where respondents work

3.2.2 Demographic data

Out of 56 respondents who completed the survey, 82% were male and 18% female, which reflects the male-dominated character of the industry. There are a number of ways in which data about gender could be considered in a study about reporting non-compliances in the nuclear/radiological field. For example, Miceli [16] in her work summarized the existent research argument about the importance of the gender variable on the propensity to blow a whistle. She pointed to some studies which assert that '*women are more likely than men to blow the whistle*' [16] due, as some suggest, to their '*lower tolerance for illegal and unethical behaviors*' [Yu & Zhang, 2006 referred in 15]. Contrary to expectations that women are more likely to blow the whistle, some have found out that in fact they are less likely, due to lower managerial positions and greater risk of retaliation [15].

The idea that gender, tenure and preference with regard to the recipient of the complaint might be interrelated [referred in 17] should receive more analysis, and so far, based on our data (where the sample size is relatively small), we cannot build a consistent pattern with regard to a gender variable and, therefore, will neither deny nor agree with the statement that gender influences the reporting in nuclear or radiological organizations. However, this is something that might be interesting to explore in the future, especially, keeping in mind efforts towards the expansion of women engagement in the nuclear sphere through the IAEA policies to attract qualified female employees to work in the IAEA [see Resources for Women at 18] and activities carried out by the Women in Nuclear professional network [see 19]. Testing whether involvement of women might influence the reporting behavior in the nuclear industry, and whether gender influences proneness to select internal versus external reporting mechanisms, could bring some value added in the context of providing an opportunity to choose reporting channels that will suit all genders.

Among our respondents, we received a good representation of different age categories (see Figure **4**). The largest group (almost 33%) was those whose members are aged 35-44, followed by a group (23.6%) of people who said they are 55-64 years old. Those participants aged 25-34 and 45-54 formed groups which are the same in size (each 18.2%). Professionals who are older than 65 comprised 7.3% of the respondents.

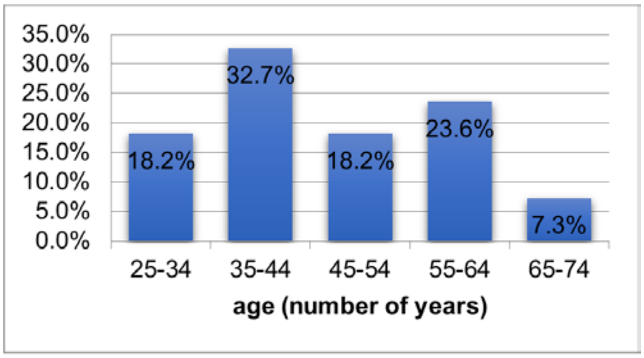

Figure 4: Age of respondents

Similar to the research data that focused on organizational tenure, studies about the age variable concluded that older members of organizations are more likely to report wrongdoing than their younger counterparts, which is explained by their better understanding of , the systems of control and their greater authority within the organizations, leaving them less hesitant to blow the whistle [summarized in 15]. On the other hand, elderly individuals who have extensive work expertise and experience in some situations may have second thoughts about reporting for fear of being forced into retirement as most likely reprisals.

The result showed that most of our respondents received a higher education, with almost 20% being holders of doctoral degrees (see Figure **5**). Around 70% of the participants have master degrees, 7.1% -bachelor degrees, and the remaining 3.6% are evenly split between vocational and other training.

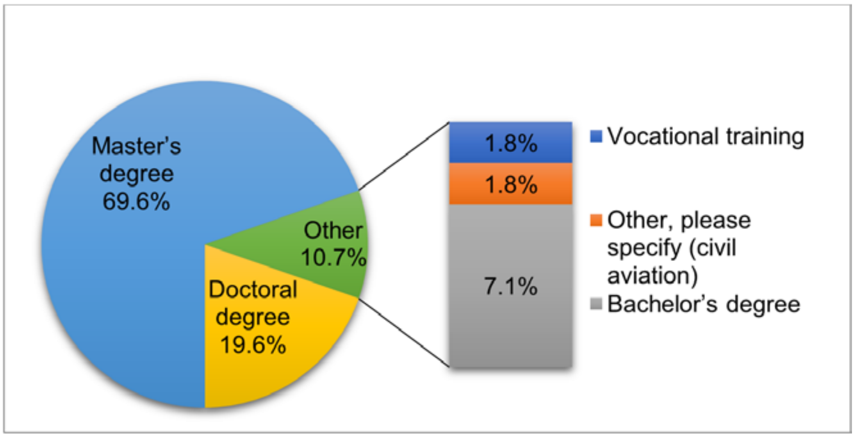

Figure 5: Level of education of the respondents

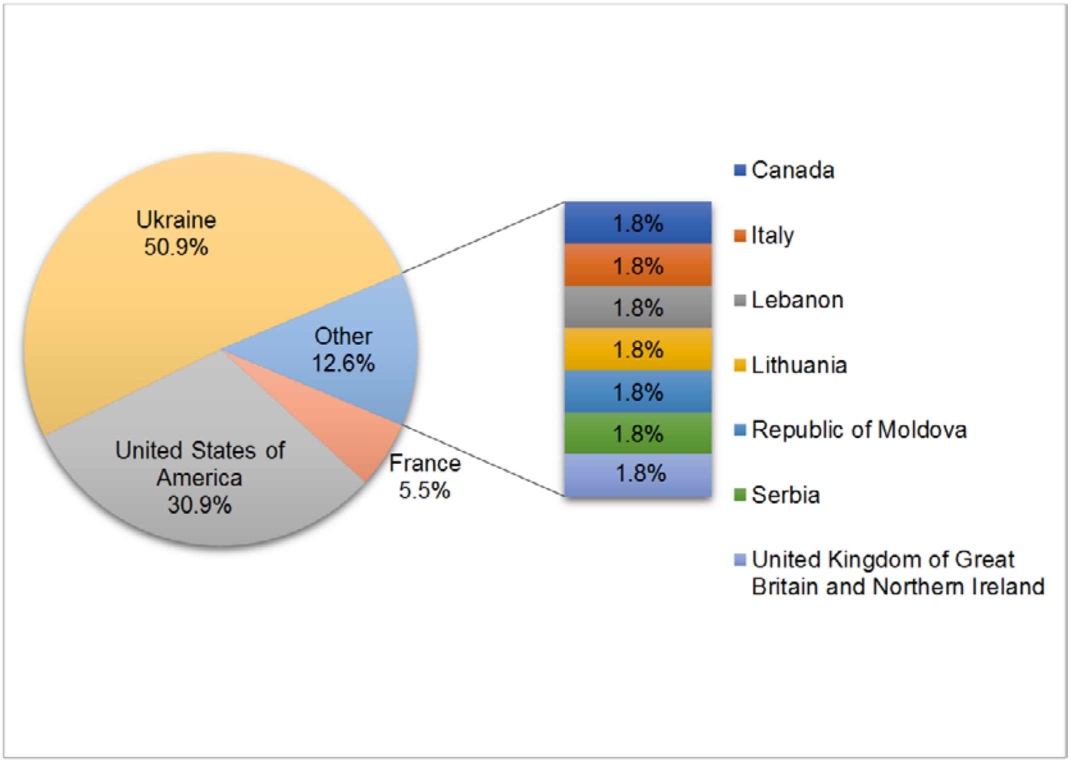

Figure 6: Nationalities of the respondents (N=55, 1 person skipped the question)

Caillier [20] suggested that '*more educated employees are expected to be more likely to blow the whistle than less educated employees, for the reason that the former may have a greater ability to find a job elsewhere if they face reprisals*'. Since in our case almost all of the respondents are relatively highly or highly educated, we will not attempt to draw conclusions based on differences in the respondents' educational level.

We tried to get responses from representatives of different nations, and therefore did not limit distribution of the survey to participants from particular nations; nonetheless, the fact that the survey was available only in the English and Russian languages limited answers to the survey to only those who speak one of these two languages.

The data on citizenship of the respondents is shown in Figure 6. More than half (50.9%) of respondents said they were Ukrainians, 30.9% indicated they were Americans, French persons constituted 5.5% of participants, and the rest (12.6% in total) was evenly split among citizens of Canada, Italy, Lebanon, Lithuania, Moldova, Serbia and the United Kingdom. As can be noticed, the profile of countries is quite diverse, although two major groups based on the country of citizenship can be singled out: Ukrainians and Americans. This, we believe, can be further explored in comparative analysis of some of the results of the survey; in particular, it can be tested whether there is any correlation between an attitude towards whistle-blowing and nationality.

Different researches have acknowledged a mediatory role of national cultural characteristics on whistle-blowing. For example, Miceli et al. [14] warned that research on whistle-blowing done for North American settings '*may not generalize to other cultures, nor even to* [all] *areas in North America*'. A comparison of whistle-blowing on the cultural level was done by Keenan [21], who examined American and Indian managers' propensity to blow the whistle. Ahmad et al. [15] looked at Malaysian whistleblowers in connection with the theory of prosocial behavior. Considering all of this evidence, it seems that attention to culture as a societal environment is a promising field for new discoveries in the complex whistle-blowing problematics.

4. Findings and their interpretation

4.1 What does a violation leading to a security breach entail and what constitutes wrongdoing?

There has been recognition among researchers that '*individuals differ in their perception of what constitutes wrongdoing*', thus some of them might go unnoticed [22]. Lack of security standards in the nuclear field exacerbates the problem with definitions of wrongdoing, since an organization should establish its own security measures based on the design basis threat. Prima facie, wrongdoing in nuclear security can be described as an act initiated from outside or within an organization that bypasses or contravenes security policies, practices, or procedures. However, some may take a deeper view that loopholes or gaps in security constitute a breach in security by revealing a weakness that can be exploited with a malicious intent. Therefore, a starting point of our investigation of reporting procedures in the nuclear or radiological industry was to determine

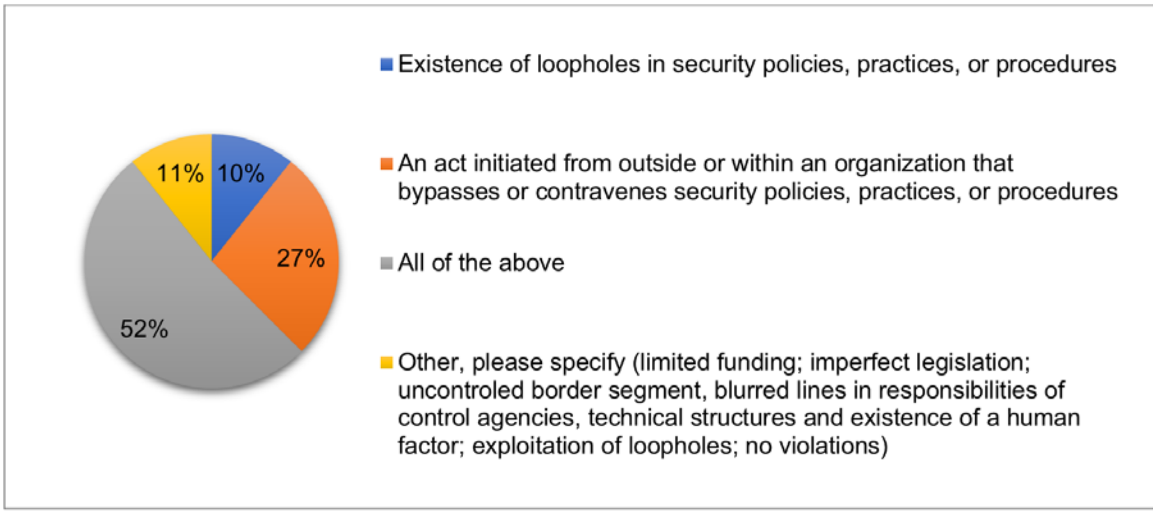

Figure 7: Perception of a violation by the respondents

how our respondents understand a violation that could lead to a security breach. The question itself might provoke certain misinterpretations; therefore, apart from providing possible options to choose from for an answer, we left room for the respondents to suggest their own answer that might best reflect their judgement. The results of the replies are presented in Figure **7**.

The majority of respondents (52%) hold a comprehensive definition of violation, which includes both: an act of an insider or outsider that contravenes security policies, practices and procedures, as well as existence of loopholes in security policies practices and procedures. On the other hand, 27% of the respondents believe that the definition of a violation should be restricted to an act initiated from outside or within an organization that bypasses or contravenes security policies, practices, or procedures. Ten percent argues that loopholes in security policies, practices or procedures are the reason for violations that lead to a security breach.

This inconsistency may be related partly to a matter of linguistics; however, individual assumptions will also affect it. Semantically, one could assume that there is a difference between a wrongdoing and a violation. If the former entails an activity or instance of doing something '*illegal, illegitimate or immoral*', the latter, one could suggest, encompasses not only an act but also a condition that is being violated or leads to a wrongdoing, or in some cases creates favorable conditions for a wrongdoing. For example, nonworking cameras at the Y-12 security complex was a clear violation of security procedure. A U.S. DoE report [23] acknowledged that one critical camera with a view on the penetration area was out of service for almost six months, which contributed to '*delays in assessing alarms and identifying the trespassers*' [23]. Still, one may describe it not as an act but rather the lack of an act or a negligent attitude to security policies that allowed anti-nuclear activists, allegedly followers of the Plowshares movement [24], to break into the premises of the Y-12 complex where nuclear weapons-grade uranium was stored [23].

Another example of loopholes could concern the existence of human reliability programs. In some countries, the presence of such programs would be prescribed by law, while others might not have such regulations. In the latter case, it will not considered a violation for a non-vetted person to receive access to sensitive nuclear material. Thus, the answer to the definition of a violation will to a large extent depend on how one regards the issue of security, which is largely conditioned by the environment in which one is living.

In addition to the organizational or individual perception of violation or wrongdoing, the cultural setting can provide its own influence on the understanding of the term. In that regard, Miceli et al. [14] posited that definition of what constitutes wrongfulness may vary from country to country. For example, giving valuable presents or money in some countries is considered as a cost of doing business [14] or as act of 'gratitude', whereas in other cultures this is classified as bribery and is totally unacceptable.

In our case, there was not any clear pattern revealed in terms of a nationality-based preference for definitions of a violation. The replies were distributed more or less equally between different categories of answers by representatives of different countries. However, we would suggest listing all answers that people provided in the 'Other' section, where some interesting observations can be made. One respondent (USA) claimed that '*the existence of*

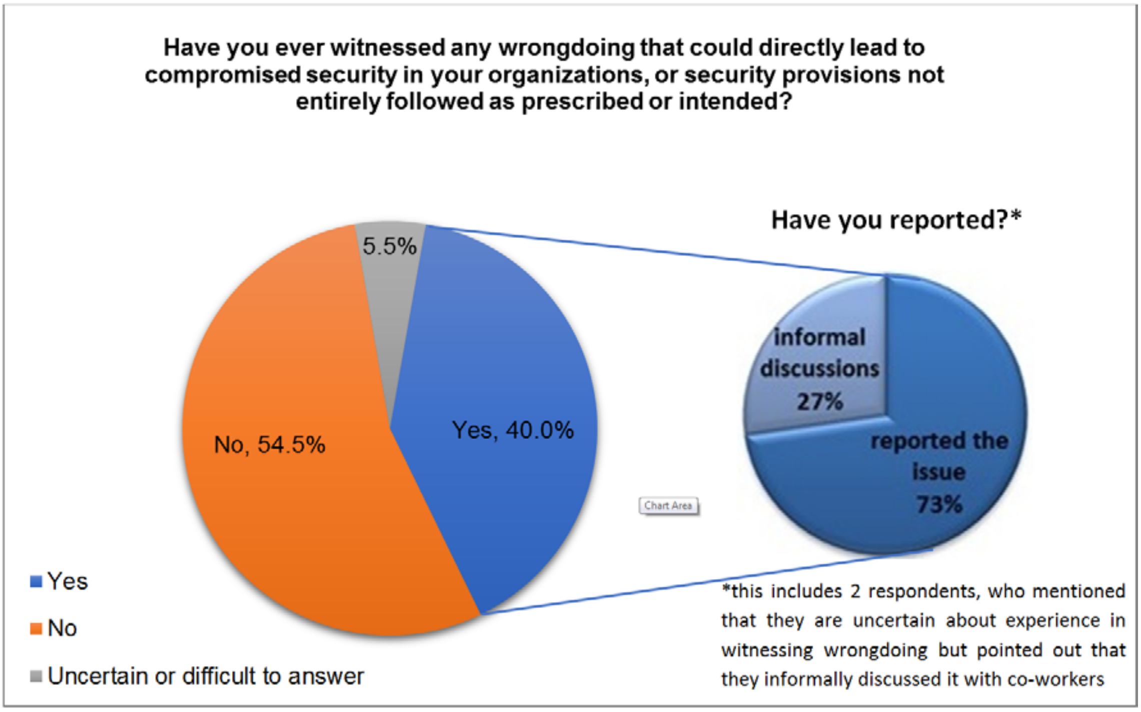

Figure 8: Experience in witnessing any wrongdoing and reporting

loopholes is not the violation, but the intentional exploitation of those loopholes. There will always be gaps to be exploited.' Another person (Ukraine) believed that '*no violations exist*', probably meaning that he has not yet experienced them in his practice. Some other answers pointed to drawbacks and weaknesses in security procedures and policies such as: '*limited funding*' (Ukraine), '*shortcomings in the legislation at the current stage, lack of highly professional staff, lack of funding*' (Ukraine), '*uncontrolled territory of the border*' (Moldova), '*blurred responsibilities among controlling organs, human and technical factors*' (Ukraine).

4.2 Experience with witnessing wrongdoing and reporting on it; the underlying reasons for reporting

It is hard to deny that whistle-blowing is a challenging and risky enterprise. A person who witnesses wrongdoing can raise an issue about an organizational problem, foster a solution to it, or vice versa, disrupt the functioning of legitimate activities [25] if, for example, allegations are not well-grounded. We asked our respondents about their experience in observing wrongdoing or security provisions not followed as prescribed or intended and whether this observation spurred them to report. The results of the survey on these questions are presented in Figure **8**.

The chart depicts that the majority (54.5%) postulated that they have not experienced witnessing any wrongdoing or neglect with regard to security procedures in their organizations. Forty percent of the respondents admitted that they have been faced with a wrongdoing or improperly followed security procedures, while a few (5.5%) expressed difficulty or uncertainty in answering such a question.

All those who answered positively to the question about witnessing a wrongdoing stated that somehow they called attention to the issue, either through informal discussion (27% - this includes two answers of those who were uncertain about whether they saw or not the wrongdoing etc.) or reporting (73%). Differentiating between two types of actions (i.e. reporting and informal discussions) is commonplace in the academic world, where the latter (informal discussions) is not equated to whistle-blowing. Miceli and Near [26], well established researchers in the area of whistle-blowing who insist that discussing informally with co-workers or family members is not reporting, build their argument on the fact that only discussions with those who might influence or affect the situation (i.e. to bring changes) constitute whistle-blowing.

To operationalize further the motives of those who have reported on alleged wrongdoing etc., we asked our respondents to select all factors from among those listed in the survey that have motivated them to report. The scale of responses is depicted in Figure **9**. Amongst all motives, one that was selected a substantial amount of times (43.5%) was the reason that '*Security is everybody's responsibility and I feel obliged to report*'. Thirteen percent of employees contended that '*A negligent attitude towards one's duties is detrimental and I did not want to work with people who do not align themselves with organizational standards*'. The same degree of response (6.5% each) was given to such reasons as '*The person in question might have had more detrimental motives in mind' and 'I was particularly worried about the risk of terrorism against my country or organization*', which indicates an acute

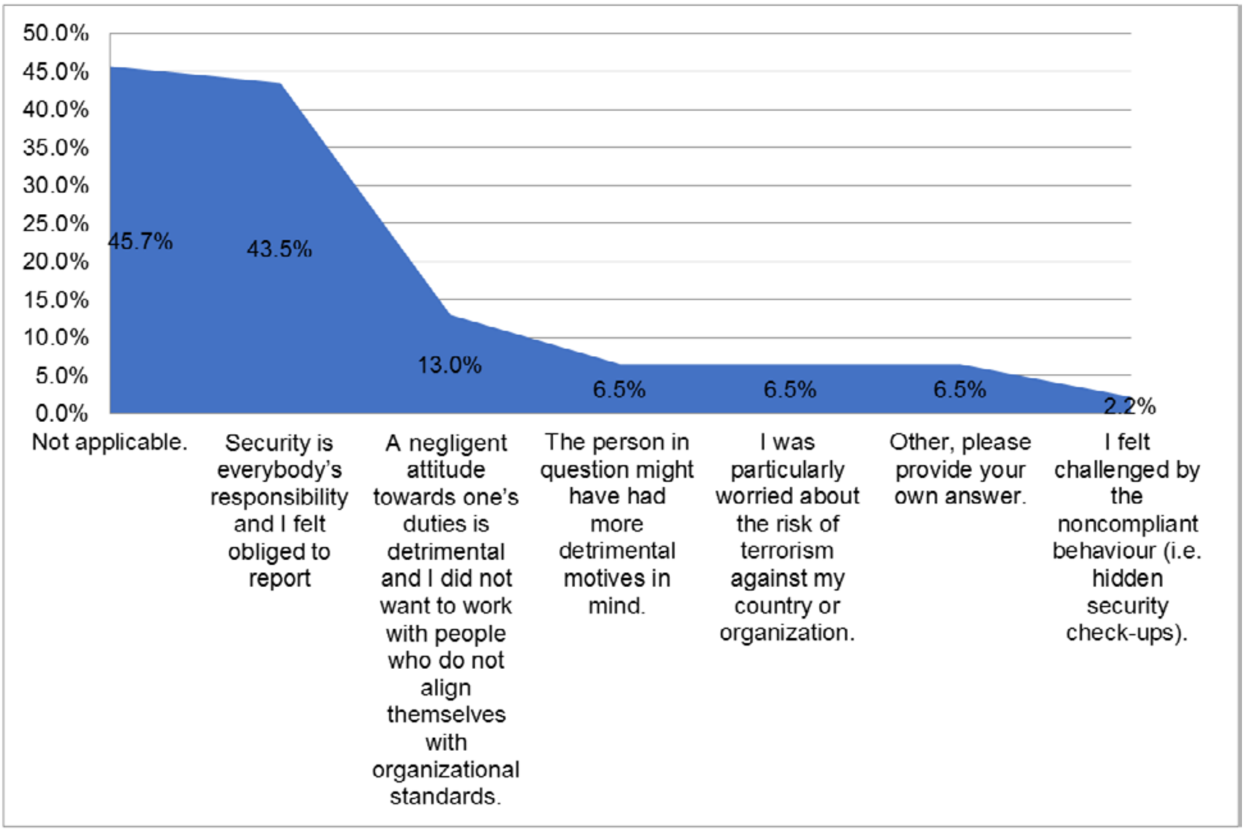

Figure 9: Factors that motivated reporting

perception of threat that potentially could concern nuclear or radiological materials handled by organizations, where respondents who have chosen these types of answer work.

Those who answered this question had a choice to provide their own explanations as well. We provide below the list of responses in the 'Other' section (6.5% selected this option) for the attention of the reader.

These '*Other*' responses include such statements:, '*I was part of a project which provided material control and protection oversight and we were responsible for monitoring, reviewing and reporting the results of our findings to those facilities where we were engaged*' (USA), '*Violations usually dealt with wrong exploitation of equipment and my duties concern the arrangement of uninterrupted working conditions*' (Ukraine), '*There is no such thing as not important issues in security; wishful thinking is the biggest enemy*' (Ukraine). One person stated that '*To report about violations is among my professional duties*' (Ukraine).

In that regard, there have been some discussions in the literature about whether to recognize reports that are considered to be part of a job description as whistle-blowing or not. An interesting observation was made by Dozier and Miceli [25] who posited that even if job descriptions require uncovering of violations, '*enthusiastic pursuit of this goal may not be rewarded in the organization*'; therefore, an individual may sometimes come into dissent with established 'organizational norms' when reporting misconduct. In this context, an exemplifying case is that of Richard Levernier, a nuclear security professional with more than 20 years of work experience, who reportedly pointed out that the possibility that suicide terrorists would not need to exit from nuclear facilities was overlooked by contingency planning scenarios [27]. After reporting as part of his job on weaknesses in security systems at nuclear power plants, he allegedly was reassigned to administrative work [27]. Numerous cases are described in the literature about employees going public when the organization fails or is unwilling to correct wrongdoing; in some cases, where they reveal weaknesses in an organization's system, they are faced with retaliation.

We also would like to indicate some factors that have influenced some people who participated in our survey not to report the issue or an alleged wrongdoing but to discuss informally with co-workers. In particular, they indicated that: '*Minor violations are better dealt with internally...*' (France) – this probably means that the person discussed the issue internally in contrast to external reporting, '*Knowledge that there is no solution for correcting a situation or it will require insurmountable financial and human resources from my organization*' (Ukraine), '*I am not in a position to personally witness security violations. As a researcher, I only learn of such issues after they've happened*' (USA), '*It was not direct wrongdoing, but rather lack of strong security culture/awareness and/or*

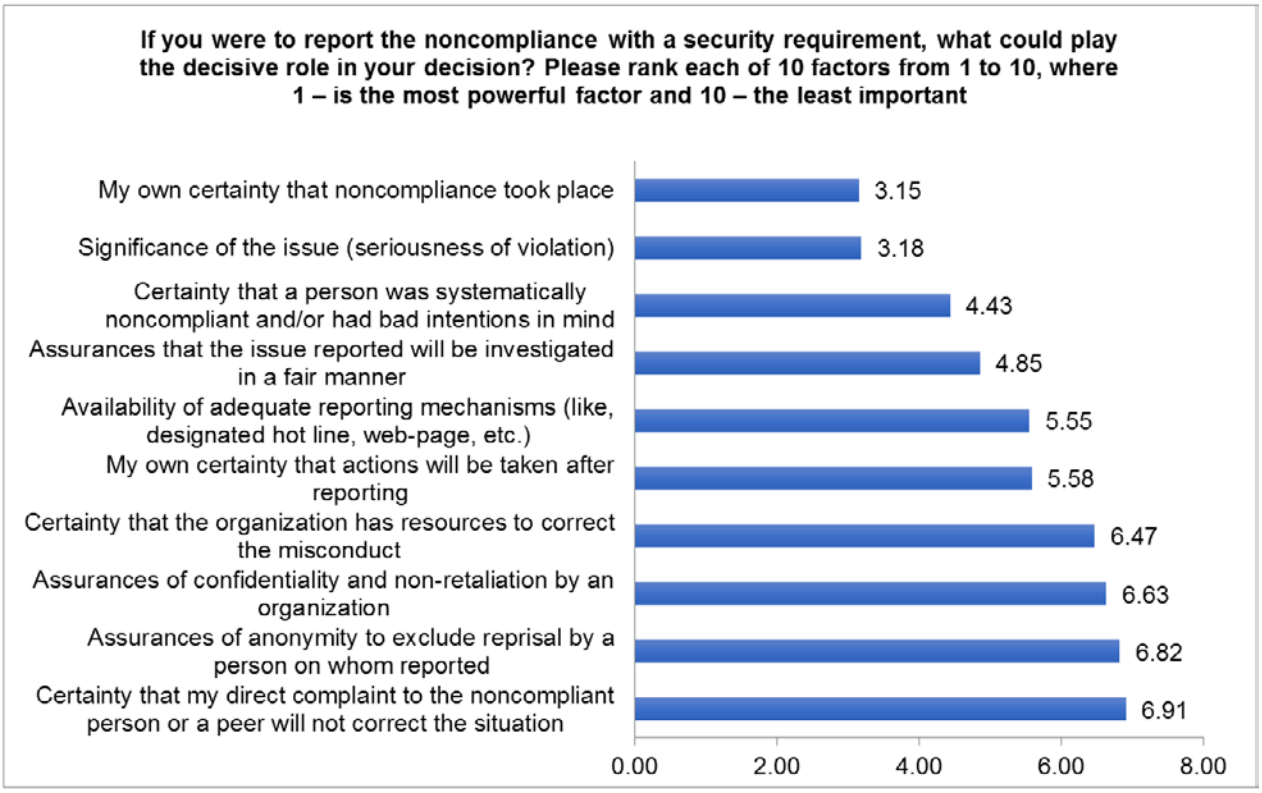

Figure 10: Drivers for reporting (determinants of intent to whistle-blow)

a compliance-based culture as opposed to a principle-based culture. Nothing really reportable' (USA), '*The issue was minor and could not affect security within the organization*' (Ukraine (5 persons), USA (1 person)), '*Belief that no action will be taken if I report*' (Ukraine). Some of the respondents from Ukraine just referred to a particular requirement in their national legislation (the piece of legislation mentioned by them concerns coordinating co-operation between governmental bodies in the event of detection of sources of ionizing radiation in an unauthorized possession, rather than speaking about reporting procedures inside an organization).

4.3 Drivers for reporting (determinants of intent to report)

We asked respondents (hypothetically if they were to observe noncompliance with a security requirement) to rank in the order of importance factors that might influence their decision to report. Although some of the rankings were missing from some of the applications, the aggregate picture looks as follows (see Figure **10**).

On average, for most of the people, ***certainty that noncompliance took place*** was the most significant determinant of an intention to report. Rationally, it can be explained by precautionary measures taken before denouncing something that may not correspond to reality, thus generating a 'false alarm'. Hence, most of the respondents are restrained from ungrounded accusations. Study of Miceli and Near [28] illustrated that '*convincing evidence that noncompliance took place*' can affect whistle-blowing behavior. As for future research, it might be interesting to study how certainty about the violation or wrongdoing is formed. In some cases, disconformity or divergence from security procedures might be clearly observed and wrongdoing might be apparent; in others the activity might be questionable; moreover, as Gundlach et al. [29] noted, wrongdoer manipulation tactics (like, 'false apologies' etc.) might reduce certainty and influence a decision to blow a whistle.

The ***significance of the issue (seriousness of the violation)*** has a strong positive relationship with the likelihood of reporting about a violation or wrongdoing. This was confirmed in our study, where this factor holds the second position in order of importance for its potential of triggering reporting behavior. In accordance with that, the results obtained in a study of U.S. federal employees showed that salience of the wrongdoing (which means that it was '*either very serious or very frequent*') has a strong influence on the likelihood of reporting by those who witness it and who hold the evidence [30]. As for the definition of seriousness of a wrongdoing, intriguingly, scientists have found that individuals on average '*perceive physically harmful acts as more serious than financial wrongdoing*' since the effects of the former usually can have a direct link to the risk posed to human health [31]. When the issue seems less serious, Keenan [32] posited that organizational propensity, which includes the amount of encouragement to report, will play a decisive role in whistle-blowing. Of course, it will also depend on how an organization tolerates wrongdoing, if, as Miceli and Near [26] noticed, it '*doesn't discourage wrongdoing* [, it] *would probably also not discourage retaliation*', which, one would assume, will increase the expected costs of reporting.

If observing a violation, there is reason for one to suspect ***bad intentions in a wrongdoer,*** this may foster a decision to report, but here we should remember the crucial role of certainty that non-compliance took place and the degree of seriousness of the violation. Barnett, Bass and Brown [33] studied how our own ethical judgement influences a decision to report on peers. Therefore, the moral standards of an observing employee and other individual variables influence the whistle-blowing process; however, we do not explore them in our study. A lot has been done in that field by other authors [see 33, 34, 35]. Our findings, which showed that certainty about wrongdoing taking place, its seriousness and the ***systemic nature of non-compliance*** of a wrongdoer are the most powerful triggering factors of whistle-blowing behavior in organizations that handle nuclear or radiological materials, are, in general, in line with the results of investigations carried out in other professional networks [28].

Assurances that the issue will be investigated in a fair manner, as well as that actions will be taken after reporting, were quite important (at fourth place) to the employees who took part in our survey. Here we would like to draw upon an example from Sandia National Laboratories to demonstrate a lack of fair investigation after breaches in security were reported by an employee of an organization that deals with nuclear materials. When Shawn Carpenter informed his superiors at the Sandia lab about systematic cyber espionage on major U.S. defense and military government agencies and their contractors, he was faced with an order to keep this secret to himself, since the computers attacked did not belong to the organization in question but to other governmental bodies and literally were assumed to be other persons' business [36]. 'Disobedience' and the subsequent external report of Carpenter resulted in his security clearance being revoked and termination of employment [36]. Evidence of reluctance from the side of organizations to investigate the issues raised by concerned employees can easily dissuade some from internal reporting or instigate them to public disclosure of violations. In contrast to that, perceived higher levels of organizational justice are positively associated with internal whistle-blowing behavior [37]. Hence, one may conclude, if the organization is not trusted, and is believed not to treat an issue in a fair manner, this may provoke silence even about salient violations or, conversely, disclosure of acts to the media or other external parties.

Experience and knowledge about reporting mechanisms influence reporting behavior [22]. This applies when they exist and employees are familiar with them, but what if no such special reporting mechanisms are established to deal with nuclear security in an organization? To receive an answer to this question, we asked our respondents to assign a ranking criterion for ***availability of complaint channels (adequate reporting mechanisms) such as designated hot line, web-page, etc.,*** based on the role it would play in motivating them to report an observed alleged wrongdoing. Our respondents placed it in the top five of the factors (out of ten). In our view, this is quite high in the ranking, which agrees with the statement that '*open-door policies, telephone "hotlines" and formal "whistle-blowing procedures" are* […] *likely to have a strong influence on individuals' decision whether to report perceived wrongdoing*' [33]. In the study by Glynn and Bunn [2] on the casino and pharmaceutical industries, they provided an example that in a number of casinos, anonymous tip-lines were an effective mechanism to enhance a security program; this could be borrowed for the nuclear security field. Establishing international 24/7 toll-free hotlines is becoming commonplace in some multinational corporations for establishing contact with a whistle-blower or those seeking advice regarding the reporting procedures to be followed; the latter may, if desired, remain anonymous [14]. Setting up such internal communication channels, as Barnett [38] contends, '*may increase the likelihood that employees discuss such concerns internally*'.

Next in the ranking of the determinants of reporting behavior, respondents of the survey put ***certainty that actions will be taken after reporting.*** A 'sleeping guard' case, as we call it, can serve as an antagonism of what a person who decides to report expects from an organization. When an employee, Kerry Beal, discovered that his colleagues in the security team at the Peach Bottom nuclear power plant in Pennsylvania took '*regular naps in what they called 'the ready room''*, he reported to supervisors, who allegedly told him '*to be a team player*' [39]. Resorting to the regional office of the Nuclear Regulatory Commission also did not bring the anticipated relief, since the plant owner to whom the issue was transferred '*said it found no evidence of guards* [being] *asleep on the job*' and the matter was considered concluded [39]. Obviously, transferring the issue to the organization, where security was not upheld, carried a risk of the issue being covered up and no corrective actions taken. Management of organizations in the nuclear and radiological field should bear in mind that such an indifferent attitude towards reporting is a manifestation of lax nuclear security culture and not something a vigilant employee who conveys a concern would expect to exist within his/her employer. Miceli et al. [14] warned that an unwelcome attitude from managers frequently deters employees from speaking up about observed wrongdoing; '*they believe nothing can or will be done to correct the problems; and* […] *these beliefs are often well-founded*'.

Certainty that the organization has the resources to correct misconduct was considered to be a factor that might influence the reporting behavior of the employees in organizations that handle nuclear or radiological materials. As per the survey results, it occupied a somewhat intermediate position in the ranking of importance. Shockingly, as Bunn et al. [40] noted, if an organization is constrained financially, it might discount or even punish employees who try to enunciate security concerns.

Interestingly, by putting ***assurances in anonymity and confidentiality to exclude retaliation*** lower in ranking, people expressed less confidence that the presence of these measures would encourage them to blow the whistle. This might lend support to the theory of public service motivation (which will be discussed later in our paper); according to which individuals in public service (and most of the organizations that handle nuclear or radiological materials in the countries we examined were government-owned) are conducive to altruistic, public service motives also associated with self-sacrifice [20].

In addition to that, Brewer and Selden [34] posited that, in general, '*whistle blowers are probably less concerned about job security*'. Furthermore, a significant body of empirical research proved that overall retaliation will not suppress whistle blowing [34, 38]. Although the fear of retaliation does not necessarily dissuade an individual from the decision to blow the whistle, it may instigate an employee, as Caillier [20] asserts, to blow the whistle externally where he or she might hope to find a refuge from punitive measures by an organization. Nevertheless, assurances of anonymity and confidentiality may still encourage some employees to communicate their concerns internally and thus, we believe, should be carefully considered in organizational policies.

Finally, last in the ranking was ***the certainty that direct complaint to the noncompliant person or a peer will not correct the situation.*** Sometimes if a person approaches a wrongdoer, the latter might acknowledge an act of noncompliance '*by using excuses or justifications*', showing that it was rather an exception than a usual practice [29]; however, based on stories of professionals in the radiological sphere, those who raise the issue are quite frequently mocked or even threatened by a wrongdoer.

4.4 The ideal recipient of the report

Profound studies have been conducted on the variables that influence what path for reporting, internal or external, an individual who observed a wrongdoing will choose [see 4, 15, 16, 17, 22, 28, 37, 38, 41, 42]. This question can be inextricably linked to organizational factors such as perceived trust in an organization etc. On the macro-level, this can be restricted by the reporting mechanisms prescribed by law in a specific country. For example, data from the literature indicate that '*the UK legislation requires internal reporting in most circumstances. Australian and the large majority of US statutes favor external reports*' [14]. Therefore, employer-employee confidentiality plays a greater role in the UK, than in the USA or Australia [14]. The issue is complicated, however, by the specifics of legislative provisions at the state level in the USA, where some states '*require or encourage internal reporting before the whistle-blower goes outside the organization*' [17].

The question on the 'right recipient' of the report can be not only a reason for a collision at the workplace but can even escalate to the courtroom. A case that happened in the Los Alamos Laboratory illustrates how publicizing security and safety concerns allegedly led to retaliation against a whistle-blower. This person reported on the perceived lax security in the lab with regard to access to classified information '*on the timing, destination and security arrangements for transport of nuclear-weapons materials to the laboratory*' by uncleared employees [43]. After the perceived failure of Los Alamos managers to correct the '*systemic problems*', Gutierrez, the whistle-blower in question, decided to go public and reported the issue '*to federal lawmakers, to a nuclear watchdog group suing the laboratory and to three New Mexico newspapers*' [43]. Despite the fact that the court ruled that federal law, i.e. the Energy Reorganization Act, '*supersede*[s] *Los Alamos policies against lab workers having unauthorized communication with government officials and the media*', all Los Alamos lab employees were 'reminded' after the ruling on the prohibition on communicating with lawmakers '*on lab issues* [which] *could be construed as lobbying or could otherwise harm the lab*' [43].

Interested in whom the respondents would trust to accept their complaint, we asked them '***If you were to report security non-compliances, who is the ideal recipient of the report? Please list all options in the order of preferences from 1 to 6***'. By asking such a question, one could assess the reporting preferences and ultimately predict employees' behavior. Based on the answers we received, some tendencies might be discerned (see Figure **11**).

The responses indicate that in nuclear or radiological organizations, supervisors are looked upon most favorably as the recipients of the claim. This is followed in the list of preferences by the head of the organization or a special control body in the organization. This data coincides in findings with other research where informants refer the issue to the immediate supervisor first [44]. King [44] explains this by both, 1) established reporting channels within the organization and 2) relational distance between employees and upper management who might not be aware of the specifics of the problem. Overall, the results of our survey show the clear preference to contain an issue within the organization, as the first two preferred reporting channels belong to the organization. Then are followed by a specialized governmental body – 3rd place.

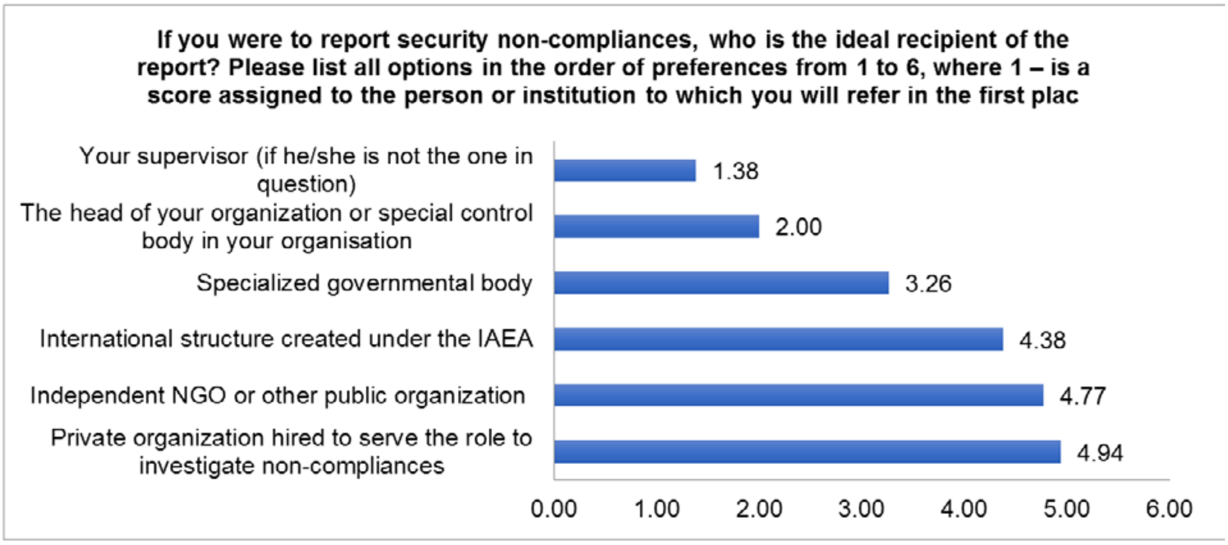

Figure 11: Preferred recipient of the report

Regarding a specialized governmental body one would mean a governmental organ intended to oversee security and receive complains on its violations. In Ukraine, for example, the National Anti-Corruption Bureau of Ukraine or NABU was established in 2014 as a law enforcement anti-corruption agency, which investigates corruption in Ukraine and prepares cases for prosecution. Therefore, a person in Ukraine can (anonymously if one so wishes) report to NABU an event where high officials abuse or misuse their authorities for gain or personal preferences. An international structure created under IAEA took the 4th place (we hypothesized about the existence of such to see if the responders would prefer this channel); the 5th place is occupied by an independent NGO or other public organization, and the last in the list of preferences is a private organization hired to serve the role of investigating non-compliances.

Miceli and Near [45], relying on previous research, condensed information on possible motives of internal reporting to two most powerful factors that can be explained by 'deviance' or 'differential association' theories. According to the first theory, choosing a supervisor or structure within an organization as the primary recipient for a complaint is explained by minimized risk associated with reporting to internal channels in comparison to an external one [45]. The latter theory accounts for '*norms of loyalty*', meaning that the climate prevalent in organizations '*is generally antagonistic toward exposing misconduct* [externally]' [45].

In that regard, Barnett [38] concluded that the consequences of external whistle-blowing are more severe '*both for organizations and whistle-blowers*'. For the former, it inflicts significant reputational damage, while for the latter it imposes risks of retaliation due to public enunciation of the violation [38]. In general, internal reporting hinders the employer-employee relationship the least and provides the opportunity for earlier correction of violations [30].

From an organizational policy perspective, Lavena [42] postulated that a supportive environment within an organization, where a supervisor is trusted by employees, contributes to a decrease in external reporting. If an organization does not tolerate dissent, thereby suppressing internal disclosure, whistle-blowers might speak out and report externally [17]. The finding that organizational size might be mediating the reporting paths - the bigger the organization, the greater the chances of external reporting, because, as suggested by Barnett [38], '*bureaucracies do not foster ideal environments for effective upward communication*' - should be considered in large research and development organizations, and in industrial settings dealing with nuclear and other radiological materials.

Summarizing what we have discussed before, there is a definite value in establishing clear reporting policies within an organization. At the same time, such policies should not be restrictive; instead of instilling fear in employees for escalating a complaint into a public domain, managers should treat security reports seriously and build a participatory work environment, characterized by solidarity, engagement and openness.

4.5 Attitude regarding those who report

By replying to the question, 'What, in your opinion, best describes to the profile of people who report security non-compliances?' 83% of the respondents have chosen an answer that says **'They are everyday people who really care about security in their organization and the nuclear community as a whole'** (see Figure **12**). Therefore, most of the respondents to our survey do not consider whistle-blowing to be a deviant behavior. Here we should admit that, although in our analysis here we use the term whistle-blowing, in the survey we have purposefully decided to avoid using this word and used the term report/reporting instead. This is partly because of the dramatism that could surround the term. Another reason is the

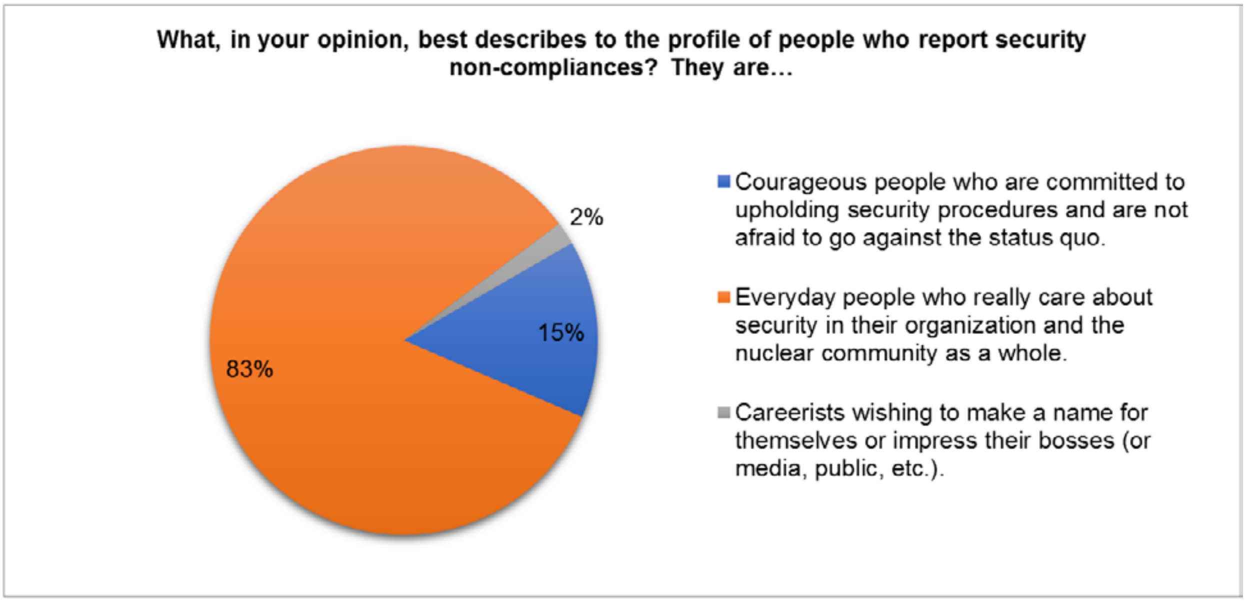

Figure 12: Attitude to those who report

controversy that exists in some countries with regard to translation of the word whistle-blowing and its ambivalent, often negative, meaning, which will be discussed in greater detail below. In that context, we used the word reporting, which is more of a neutral term and does not bring negative connotations. Thus, it allowed respondents to answer questions without being influenced by any painful historic narrative and to assess the act of reporting rather than an attitude towards the word.

Seeing reporting or whistle-blowing as a normal, not extraordinary behavior seems to be in line with one strand of argument in the literature, according to which scholars assert that '*whistle-blowers have not been found to be especially "moral" people, "religious" people, "political" people, or "socially responsible" people*' but ordinary people who decided to make it their business and to act '*regardless of their own good*' [46]. Another possible explanation for the fact that a majority of the respondents see whistle-blowing as an ordinary act could deal with a self-reporting bias, as noted repeatedly in the literature about whistle-blowing. Thus, respondents do not reveal their true feelings if asked directly on the subject but try to choose the answer which might seem rational to them or socially acceptable [34]. Therefore, in line with proclaimed values of being observant, the respondents might have chosen the answer that seemed right to them and would correspond to a strong security culture. To minimize the effect of self-bias, we would recommend asking additional and probing questions, including requests to the respondents to assess actions described in short vignettes. Doing this, however, would require large investments of time and not every employee in the nuclear sphere would consider dedicating his or her working time to filling out such a survey.

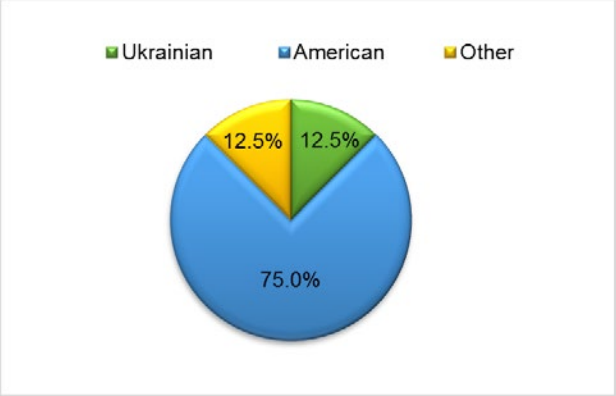

Figure 13: Nationalities of respondents who characterize people who report as "courageous people who are committed to upholding security procedures and are not afraid to go against the status quo"

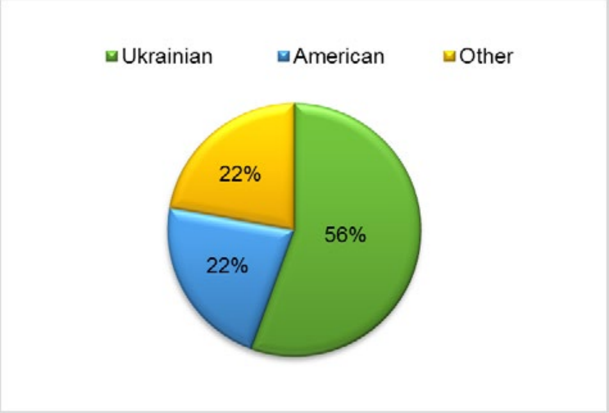

Figure 14: Nationalities of respondents who characterize people who report as "everyday people who really care about security in their organization and the nuclear community as a whole"

Interestingly, however, some eight respondents (15%) to the survey, six of which (constituting 75 percent) were Americans, one Ukrainian and one Lebanese, held the view that reporting security non-compliances is a characteristic that is attributed to ***'Courageous people who are committed to upholding security procedures and are not afraid to go against the status quo'*** (see Figure 13). Some possible explanations for this phenomenon might be as follows. First, we assume that the respondents might be influenced by the number of media coverages about whistle-blowers in the nuclear industry who became disadvantaged after reporting incompliances or revealing nuclear safety or security weaknesses. Due to the fact that the media, especially in the USA, had covered a lot of such dramatic and often unfortunate events (albeit retaliation is not as frequent as might seem from the media [26]), this might contribute to a feeling of self-sacrifice and courage that whistle-blowers allegedly need to have in order to challenge the existing situation. Thus, U.S. nationals and residents might have been more aware of retaliation against 'dissident' employees than, for example, Ukrainians, where media reports have not been that frequent, neither about whistle-blowing nor on the retaliation. Secondly, some court cases in the USA have exemplified that '*the law in the United States provides inadequate protection to whistle-blowers and gives organizations too little incentive to take corrective action, providing scant reason to believe that whistle-blowers will succeed in their quest to get wrongdoing stopped (e.g., Dworkin & Near, 1997; Miceli et al., 1999)*' [16]. Finally, some of the respondents had security functions as role-prescribed, i.e. security specialist (see Figure **1**), and most of them happened to be Ukrainians; therefore they (Ukrainians) might have considered reporting of violations as a duty rather than an act of courage or disloyalty (see Figure 14**.**).

One Ukrainian, however, did not hold a high opinion of whistle-blowers, as was shown by his choosing an answer that describes people who report violations as ***'Careerists wishing to make a name for themselves or impress their bosses (or media, public, etc.)'***. For him, reporting is not a negative deviant behavior but rather an unethical one which, as Appelbaum et al. [47] explain, '*deals with the breaking of societal rules*'. One might assume that a Soviet past, with its specific usage of reporting as an act to suppress civil disobedience and gain benefits from a regime, might have stigmatized reporting procedures in post-Soviet countries. This is especially true if one considers that whistle-blowing might have a negative connotation (it is translated in the Russian-speaking post-Soviet world as 'доносительство') related to reporting to the NKVD (abbreviated from *Narodnyi Komissariat Vnutrennikh Del*, meaning The People's Commissariat for Internal Affairs) – a ministry of the Soviet government responsible for security and law enforcement and which is associated with repression. Thus, receiving such an answer to the survey from a citizen of a country which was part of the Soviet empire is not something unusual or unexpected. In general, though, there might be in any country whistle-blowers who may seek '*self-aggrandizement and publicity*' [25].

To summarize, despite the overall optimistic picture regarding the prevalent attitude towards whistle-blowing as a normal, 'business-as-usual' act, we would like to point to the disturbing number of incidences when reporting was not taken seriously and those where retaliation did take place. Therefore, agreeing with the role of training on whistle-blowing policies, ethics and organizational procedures [32], we believe a set of generic templates for communications as well as dedicated training sessions will encourage reporting in the nuclear and radiological sphere and help minimize loopholes in security.

4.6 What is needed by employees to follow security procedures in their organizations

Figure **15** reports the things that subjects of the study indicated were the most important in helping them to follow security procedures in their organizations. We asked respondents to rank six factors in the order of importance. The mean results indicate that **additional training in security procedures and clear guidance from senior management to follow the rules and management's own adherence to them were the most appreciated factors**, getting on average 2.71 and 2.74 rankings, respectively.

An example that happened in Lithuania in 1992 might be brought to the attention of the reader to showcase the importance of training on security policies. A computer programmer named Oleg Savchuk, who placed a computer virus, was sentenced in court for trying to sabotage a nuclear reactor at the Ignalina Nuclear Power Plant [48]. Allegedly, this worker was trying, in such a way, '*to call attention to a weakness in the plant's control system and then may have hoped to be rewarded for his service*' [49]. Though his true motives remain unclear, the attempt (even though maybe with a benign final purpose) to damage the facility is apparent, which clearly demonstrates the need for training, both in security procedures and whistle-blowing practices. We suggest that the latter not only will help to improve security in organizations but also may reduce the number of non-legitimate claims and deter frivolous campaigns.

In our survey, we pointed to the need for practicing skills during exercises. Glynn and Bunn [2] also suggested that brainstorming on possible diversion scenarios and responding counter efforts of security personnel, which have proven to be beneficial in the pharmaceutical business, could be used to simulate security breaches in the nuclear industry. Although a lot of similar exercises are currently run in organizations that handle nuclear or radiological

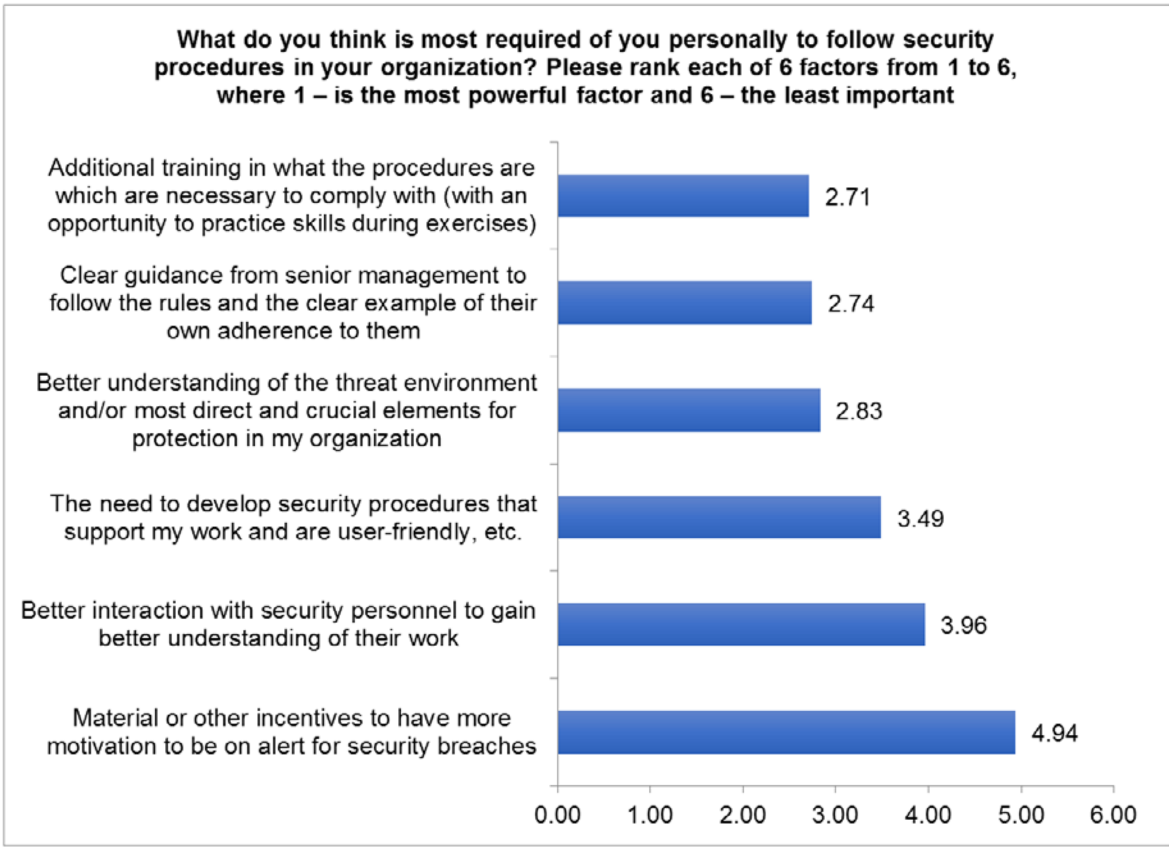

Figure 15: Things required to follow procedures

materials, the benefits of brainstorming on potential vulnerabilities and stimulation of vigilance are greater than simple usage of preset security scenarios. This will also fit into the need to give employees a ***better understanding of the threat environment and/or most direct and crucial elements for protection in their organization*** (placed at 2.84 in the ranking)**.** Although the design basis threat is a classified document, secrecy should not hamper sharing some of the information with employees; it might lead to greater engagement from the side of workers in terms of protecting critical elements and complying with procedures. Also, engaging staff members in implementing the IAEA's self-assessment methodology of nuclear security culture [50] serves as an additional learning experience, enabling workers to apply generic principles to specific needs of their organizations' security regime.

The next factor in the ranking scale, with a score of 3.49, was ***the need to develop security procedures that support my work and are user-friendly, etc.*** One may suggest that this is especially relevant in the cyber-dimension of nuclear security. There was a case described by the media, where Edward McCallum, the former director of safeguards and security programs of the U.S. Department of Energy, was cited saying that many laboratories that deal with nuclear materials or perform research on them resist introduction of new network security architectures and procedures, since they perceive them as '*unnecessarily expensive and a hindrance to operations*' [51]. This attitude shows that a special effort should be made to explain the importance of newly-established procedures and increase their user-friendliness.

With regard to the ranking in our survey, the fifth place was taken by the **better interaction with security personnel to gain better understanding of their work.** This can be closely related to training activities and empowerment actions described above; however, it also implies narrowing of the communication gap between the security unit and other personnel. This is because a person who is not part of the facility's security contingent may think security is someone else's responsibility and that security successes and failures have little to do with anything that person does or fails to do. In this regard, a study to determine possible implications for whistle blowing in relation to the existence of professional subcultures will be useful.

Unlike Miceli and Near [22], we did not receive support for a statement that material incentives would encourage whistle-blowing. Our participants downplayed the role of ***financial rewards in encouraging them to follow security procedures and stay on alert when they are breached***. Financially rewarding security vigilance could have a negative effect, first, because people who have observed the violation may, *vice versa*, be discouraged by the financial incentives (in order not to be regarded as '*hunters for financial gain*', which might contradict their ethical principles and sometimes even cause ostracism by their colleagues); second, there also can be those who may misuse the system and reap financial gain by making illegitimate claims. With closer examination, Caillier [20] finds an explanation to the phenomenon of disregard for monetary benefits in public service motivation. The concept of public service motivation takes its roots from the *'special calling'* '*to pursue the common good and further the public interest*' [34]. Whether or not a low regard for monetary rewards is a defining feature of public-service motivation is not entirely clear, but it is definitely trivial, as Brewer and Selden [34] showed, among public employees.

5. Conclusions and recommendations

The issue of reporting on security breaches in the nuclear and radiological sector has been overlooked for a long time; the scarce discussions on the topic have usually been limited to an acknowledgement of the problem of operationalization of fair reporting in an organization's policies and lack of approaches in ensuring its effectiveness. At the same time, instances of retaliation against whistleblowers who report security incompliances or raise concerns about inappropriate security measures in the nuclear field are disturbingly frequent, as was shown by some anecdotal evidence in our work. Dworkin and Near [30] reasonably admit that '*the problem for organizations is not how to avoid whistle-blowing, but how to diminish its negative consequences and to maximize its positive aspects*'. We find that this statement extends to the nuclear and radiological sphere. Opportunities enclosed in reporting for boosting a strong nuclear security culture are huge, but so are the challenges. The task is to unearth drivers of reporting so that one can build on them, expose vulnerabilities and work on the elimination of impediments, promote raising good-faith concerns and decrease adverse factors associated with whistle-blowing. With the pursuit of this current study, we have contributed to an appreciation of the importance of this task and, hopefully, have provided some findings to be used further.

We have not encountered step-by-step guidelines on establishing reporting mechanisms on security matters in organizations that handle nuclear and radiological materials; therefore, one may conclude that they are not very common and thus need to be explored. Therefore, on the state-level, we would like to suggest looking at the areas where such exist. For example, in the chemical industry, Chemical Facility Anti-Terrorism Standards (CFATS) were adopted with the aim of improving security at high-risk chemical facilities in the USA. The recent report of the Government Accountability Office on *Critical Infrastructure Protection. Improvements Needed for DHS's Chemical Facility Whistleblower Report Process* [see 7] provides some useful suggestions on the regulatory level for fostering reporting procedures. We suggest familiarization with the lessons drawn from the chemical industry so as to avoid repetition of the same mistakes in the nuclear and radiological sphere when operating a reporting mechanism. In a long run, review of legislation in countries as well as analysis of prospects of passage in the countries where it is currently absent is warranted. Some work on the state level (for instance, for the USA) has been done by researchers [see 30], though it may require an update due to the development of legislation and subsequent changes since the time of the research.

On the organizational level, an overview of how reporting on safety matters in nuclear and radiological organizations is implemented could be beneficial. For example, in the Brookhaven National Laboratory, USA, people are given the authority to stop an activity that he or she believes constitutes an imminent danger for the environment or health. Every newcomer to the lab is trained in the Stop Work Procedure. If the threat is not an urgent one, a 24-hour hotline operates for reporting safety concerns; the voice mailbox is checked by the operator at least twice a day.

At the management level, we find it useful to consult the work of Miceli et al. [14] *A Word To The Wise: How Managers And Policy-Makers Can Encourage Employees To Report Wrongdoing*. It contains some guidance on how to encourage reporting. Apparently, effective and efficient reporting procedures will require a climate and culture change within an organization [42]. A nuclear security culture coordinator (referenced in the IAEA draft guidance) should embark on these efforts, but alone little can be done; a greater commitment from the highest level of management to the security personnel in organizations and their appreciation of importance of reporting procedures are imperative for progress in this area. All of the survey participants indicated the value of clear guidance from management on security provisions and their adherence of the latter to the rules in general. Thus, reporting procedures should be known by the staff of organizations that deal with sensitive materials and transcribed into the *modus operandi* of the organization.

Our study has shown that professionals in the field will trust their supervisors to be the recipient of their concern. Consequently, supervisors have responsibilities for actions and treating disclosed concerns with due regard. If the issue shared demonstrates a risk to other operational units or structures, the information should be transferred in confidence to the right recipient; there is no place for a silo mentality in security matters, where stakes are so high due to the danger associated with the risk of unauthorized possession of materials, their misusage or sabotage etc.

The study has shown that reporting typically is treated as an ordinary behavior of normal employees who have a strong conscience for security. However, some of the respondents still feel that this is a risky undertaking, although one with honorable intentions, whereas a minority does not believe in the good intentions of those who report but rather see it as committing an act aimed at gaining career benefits for themselves. This gives a reason to suggest that education on whistle-blowing might be well-perceived by the professional community in the nuclear and radiological area and might help address the questions they might have and ease their concerns. This is especially needed so that morale in organizations is not compromised by ineffective, incomprehensive introduction of reporting.

Our study agrees that *'finding the right encouragements or inducements for whistle-blowers might be problematic and certainly will require long term, concerted effort'* [22]. To add to this, our study has shown a rather low regard of professionals in the nuclear and radiological sphere to material incentives; the relation of this phenomena to public-service motivation theory needs to be tested.

Findings also suggest that security problems must be regarded in a complex manner. Our participants indicated on numerous occasions that imperfect legislation, the level of financing, inappropriate division of labor and blurred responsibilities etc. can compromise security in organizations.

6. Acknowledgement

We thank the Brookhaven National Laboratory Nonproliferation and National Security Department staff and Department Chair Susan Pepper, for their welcome and support during preparation and implementation of this research, and their valuable comments to the survey. The U.S. Department of Energy provided funding for the research internship, for which we are very grateful. We wish also to thank the World Institute for Nuclear Security for posting a news item on their website about the survey and all colleagues who helped with distribution of the survey. Finally, our sincere gratitude goes to all those who filled out the survey, for the dedication of their time and insights shared.

7. References

[1] Khripunov, I., *Nuclear Renaissance and Security Culture.* IFANS Review, 2010. **18**(2): p. 95-120.

[2] Glynn, K.M. and M.G. Bunn, *Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries*. 2013, Harvard Kennedy School of Government.

[3] IAEA, *Establishing a Code of Ethics for Nuclear Operating Organizations*, in *IAEA Nuclear Energy Series*. 2007, INTERNATIONAL ATOMIC ENERGY AGENCY: Vienna. p. 4.

[4] Near, J.P. and M.P. Miceli, *Organizational dissidence: The case of whistle-blowing.* Journal of Business Ethics, 1985. **4**(1): p. 1-16.

[5] Kohn, S.M. and T. Carpenter, *Nuclear Whistleblower Protection and the Scope of Protected Activity Under Section 210 of the Energy Reorganization Act.* Antioch LJ, 1986. **4**: p. 73.

[6] Jubb, P.B., *Whistleblowing: A Restrictive Definition and Interpretation.* Journal of Business Ethics, 1999. **21**(1): p. 77-94.

[7] GAO, *Critical Infrastructure Protection. Improvements Needed for DHS's Chemical Facility Whistleblower Report Process. Report to Congressional Committees*. 2016, United States Government Accountability Office: Washington, D.C.

[8] nis2016.org. *Joint Statement of the 2012 Seoul Nuclear Industry Summit*. 2016 30.11.2016]; Available from: http://nis2016.org/agenda/documents/documents-joint-statement-of-the-2012-seoul-nuclear-industry-summit/.

[9] nis2016.org. *Joint Statement of the 2016 Nuclear Industry Summit*. 2016 30.11.2016]; Available from: http://nis2016.org/agenda/documents/documents-nuclear-industry-summit-2016-joint-statement/.

[10] IAEA, *Objective and Essential Elements of a State's Nuclear Security Regime: nuclear security fundamentals*. 2013, International Atomic Energy Agency: Vienna. p. 15.

[11] IAEA, *Nuclear Security Culture. Implementing Guide*. 2008. p. 37.

[12] IAEA, *Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme. Implementing Guide.* 2013, International Atomic Energy Agency: Vienna. p. 73.

[13] Bunn, M. *Incentives for Nuclear Security (Conference Paper)*. 2005 30.11.2016]; Conference Paper]. Available from: http://live.belfercenter.org/publication/12712/incentives_for_nuclear_security.html

[14] Miceli, M.P., J.P. Near, and T.M. Dworkin, *A word to the wise: How managers and policy-makers can encourage employees to report wrongdoing.* Journal of Business Ethics, 2009. **86**(3): p. 379-396.

[15] Ahmad, S.A., M. Smith, and Z. Ismail, *Internal Whistle-Blowing Intentions: A Study of Demographic and Individual Factors.* Journal of Modern Accounting and Auditing, 2012. **8**(11): p. 16-32.

[16] Miceli, M.P., *Whistle-Blowing Research and The Insider Lessons Learned and Yet to Be Learned.* Journal of Management Inquiry, 2004. **13**(4): p. 364-366.

[17] Dworkin, T.M. and M.S. Baucus, *Internal vs. external whistleblowers: A comparison of whistleblowering processes.* Journal of Business Ethics, 1998. **17**(12): p. 1281-1298.

[18] IAEA. *Resources for Women*. [cited 2016 05.12.2016]; Available from: https://www.iaea.org/about/employment/women.

[19] WiN. *Welcome to Women in Nuclear Global*. [cited 2016 05.12.2016]; Available from: http://www.winglobal.org/.

[20] Caillier, J.G., *Public Service Motivation and Decisions to Report Wrongdoing in US Federal Agencies Is This Relationship Mediated by the Seriousness of the Wrongdoing.* The American Review of Public Administration, 2016: p. 1-22.

[21] Keenan, J.P., *Comparing Indian and American managers on whistleblowing.* Employee Responsibilities and Rights Journal, 2002. **14**(2-3): p. 79-89.

[22] Miceli, M.P. and J.P. Near, *The relationships among beliefs, organizational position, and whistle-blowing status: A discriminant analysis.* Academy of Management journal, 1984. **27**(4): p. 687-705.

[23] U.S.DOE, *Special Report. Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex*, in *DOE/IG-0868*, O.o.I.G.O.o.A.a. Inspections, Editor. 2012.

[24] Schlosser, E. *Break-In at Y-12. How a handful of pacifists exposed the vulnerability of America's weapons-grade uranium.* The New Yorker 09.03.2015 01.12.2016]; Available from: http://www.newyorker.com/magazine/2015/03/09/break-in-at-y-12.

[25] Dozier, J.B. and M.P. Miceli, *Potential predictors of whistle-blowing: A prosocial behavior perspective.* Academy of Management Review, 1985. **10**(4): p. 823-836.

[26] Miceli, M.P. and J.P. Near, *Relationships among value congruence, perceived victimization, and retaliation against whistle-blowers.* Journal of Management, 1994. **20**(4): p. 773-794.

[27] Martin, B., *Nuclear Power and Antiterrorism: Obscuring the Policy Contradictions 1.* Prometheus, 2007. **25**(1): p. 19-29.

[28] Miceli, M.P. and J.P. Near, *Characteristics of organizational climate and perceived wrongdoing associated with whistle-blowing decisions.* Personnel Psychology, 1985. **38**(3): p. 525-544.

[29] Gundlach, M.J., S.C. Douglas, and M.J. Martinko, *The decision to blow the whistle: A social information processing framework.* Academy of Management Review, 2003. **28**(1): p. 107-123.

[30] Dworkin, T.M. and J.P. Near, *Whistleblowing Statutes: Are They Working?* American Business Law Journal, 1987. **25**(2): p. 241-264.

[31] Greenberger, D.B., M.P. Miceli, and D.J. Cohen, *Oppositionists and group norms: The reciprocal influence of whistle-blowers and co-workers.* Journal of Business Ethics, 1987. **6**(7): p. 527-542.

[32] Keenan, J.P., *Blowing the whistle on less serious forms of fraud: A study of executives and managers.* Employee Responsibilities and Rights Journal, 2000. **12**(4): p. 199-217.

[33] Barnett, T., K. Bass, and G. Brown, *Religiosity, ethical ideology, and intentions to report a peer's wrongdoing.* Journal of Business Ethics, 1996. **15**(11): p. 1161-1174.

[34] Brewer, G.A. and S.C. Selden, *Whistle blowers in the federal civil service: New evidence of the public service ethic.* Journal of public administration research and theory, 1998. **8**(3): p. 413-440.

[35] Park, H., M.T. Rehg, and D. Lee, *The influence of Confucian ethics and collectivism on whistleblowing intentions: A study of South Korean public employees.* Journal of Business Ethics, 2005. **58**(4): p. 387-403.

[36] TMC-NEWS, *Sandia Hacker Gets $4 Million: Analyst Fired For FBI Contact*, in *Albuquerque Journal (NM) (KRT) Via Thomson Dialog NewsEdge*. 14.02.2007, TMC NEWS.

[37] Seifert, D.L., et al., *The influence of organizational justice on accountant whistleblowing.* Accounting, Organizations and Society, 2010. **35**(7): p. 707-717.

[38] Barnett, T., *A preliminary investigation of the relationship between selected organizational characteristics and external whistleblowing by employees.* Journal of Business Ethics, 1992. **11**(12): p. 949-959.

[39] Mufson, S., *Video of Sleeping Guards Shakes Nuclear Industry*, in *Washington Post* 04.01.2008 Washington Post

[40] Bunn, M., et al., *Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?* 2016.

[41] Cho, Y.J. and H.J. Song, *Determinants of Whistleblowing Within Government Agencies.* Public Personnel Management, 2015. **44**(4): p. 450-472.

[42] Lavena, C.F., *Whistle-blowing individual and organizational determinants of the decision to report*

wrongdoing in the federal government. The American Review of Public Administration, 2016. **46**(1): p. 113-136.

[43] Hoffman, I. *Whistleblower Wins Case Against Lab. Ruling Protects Rights Of Workers To Report Concerns*. The Albuquerque Journal 02.07.1999; Available from: http://www.state.nv.us/nucwaste/news/nn10114.htm.

[44] King, G., *The effects of interpersonal closeness and issue seriousness on blowing the whistle.* Journal of Business Communication, 1997. **34**(4): p. 419-436.

[45] Miceli, M.P. and J.P. Near, *What makes whistle-blowers effective? Three field studies.* Human Relations, 2002. **55**(4): p. 455-479.

[46] Contu, A., *Rationality and Relationality in the Process of Whistleblowing Recasting Whistleblowing Through Readings of Antigone.* Journal of Management Inquiry, 2014. **23**(4): p. 393-406.

[47] Appelbaum, S.H., G.D. Iaconi, and A. Matousek, *Positive and negative deviant workplace behaviors: causes, impacts, and solutions.* Corporate Governance: The international journal of business in society, 2007. **7**(5): p. 586-598.

[48] Potter, W.C., *Less Well Known Cases Of Nuclear Terrorism And Nuclear Diversion In Russia*. 20.08.1997, Center for Nonproliferation Studies Unpublished Paper.

[49] Ferguson, C.D. and W.C. Potter, *The four faces of nuclear terrorism*. 2005: Routledge.

[50] IAEA, *Self-assessment of Nuclear Security Culture in Facilities and Activities*. IAEA Nuclear Security Series. 2017, Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY.

[51] Verton, D. *DOE clamps down on whistle-blower for security leaks*. 10.06.1999 01.12.2016]; Available from: https://fcw.com/articles/1999/06/10/doe-clamps-down-on-whistleblower-for-security-leaks.aspx.