The Role of the Human Resources Function in the Mitigation of Insider Threats in Nuclear Organizations

Authors: Ms. Isis Leslie, Tetra Tech Inc., Mr. Matthew Van Sickle, MVS International LLC.
Mr. Patrick Lynch, Oak Ridge National Laboratory (ORNL), Mr. Cary Crawford, ORNL

Abstract

Due to its unique nature, the nuclear industry requires a highly trained, competent and trustworthy workforce. It is important to hire the right people with the right attitudes and qualifications at the right times. In this paper we aim to demonstrate how facilitating effective integration between the human resource function (HR) and other management functions will allow for the creation and implementation of and cohesive and cross-cutting strategy for identifying security sensitive positions and then ensuring that they are appropriately staffed. When properly enabled, the HR department is well placed to support the function of ongoing oversight and timely review of these security sensitive positions, and to intervene in the critical pathways to insider threat, creating choke points to prevent an employee who is experiencing difficulties from progressing through to the 'hostile act' stage. This paper examines where and how the HR function can intervene on these critical pathways, and explores these key enablers, including the role of senior management and the importance of an appropriately trained and resourced HR team. This paper also considers how HR can be used to mitigate against the siloed structures which can be an impediment to the creation of an effective insider threat programme. We also aim to demonstrate how specific Human Resource Management activities carried out by the HR department can support the development of a competent and suitable workforce and contribute to the development of an organizational culture that promotes safety and security.

The observations and good practices in this paper have been developed in collaboration with industry and academia, and drawn from a variety of countries and company cultures as well as a broad spectrum of organizational types. Any conclusions and examples of current good practice are designed to be applicable to a wide range of nuclear organizations, from power related facilities to transportation and research and development.

Summary

The key elements of the role of the department of Human Resources (HR) in insider threat mitigation over the employee lifecycle are:

- Job task analysis: providing a holistic perspective on role requirements to consider attitudes and personal predispositions alongside technical qualifications and experience;
- Recruitment and succession planning: hiring the right people with the right attitudes and qualifications at the right times;
- On-boarding and the creation of a robust security culture: ensuring new hires understand the security requirements of their role from the outset;
- Employee engagement and assistance: providing a 'safe space' to receive concerns and handle them appropriately;
- Organizational responses: ensuring the organization is perceived as a fair and inclusive place to work and responds to problems effectively;

- Performance management: providing holistic and continuing support and monitoring of employee performance; and
- Attrition: managing the exit process to maximise ex-employee satisfaction and receive organizational feedback.

Background

Over the past several years, countries around the world have been faced with the increasing possibility of terrorist attacks perpetrated by individuals claiming to have been inspired by, amongst others, religiously oriented groups like Islamic State and Al Qaeda, and by right-wing anti-government militias and white supremacist groups. From the perspective of the nuclear sector, 'one of the most serious security concerns is that employees could become radicalised—or that already radicalised individuals are hired— and subsequently use their positions of trust and authority to carry out a malicious act'[1]. In addition, due to the increasing reliance on computer systems, networks and other digital systems, security professionals in the nuclear industry are also concerned at the cyber threats posed by insiders within organizations. In these instances, disgruntled employees with access to and knowledge of internal systems, would be well situated to commit sabotage and other malicious acts, and the HR Department can be a valuable partner to identify these threats. The insider threat could also be exploited for other purposes, including but not limited to the media, organized crime or activist groups.

In addition, many countries motivated by climate change concerns and energy independence, have decided to embark on new nuclear power programs, while others, faced with waste concerns, financing and/or public opposition, are phasing out their programs. In these cases, the workforce of those organizations that are newly established as well as those that are experiencing attrition must be managed to ensure that each individual develops and maintains the correct knowledge, skills and attitudes necessary to perform required tasks consistent with the expectations of the organizations.

With this expanding and evolving workforce, the HR departments of nuclear organizations serve both as a vital pillar in ensuring that nuclear organizations are appropriately staffed and as an effective ally of the security department in ensuring that insider threat mitigation is considered from the very outset of the employee lifecycle.

Objective and Users

The objective of this project is to examine the role of the HR department in identifying job positions that are more likely to pose insider threats to nuclear facilities, and to analyze the role and function of HR professionals in mitigating these potential threats through the recruitment, hiring, on-boarding and succession planning functions. Additionally, this project will compile good practices related to human resource management that can be used to support the development of more robust organizational cultures, and subsequently, the mitigation of insider threats.

This will help to facilitate an increased ability for nuclear organizations to identify and mitigate potential insider threats through the enhanced involvement of human resource professionals. We aim to host an international meeting that will help us compile a sample framework and good practices that will support

---

[1] World Institute for Nuclear Security (WINS) Workshop on Countering Violent Extremism and the Insider Threat in the Nuclear Sector, London, UK. 3-5 December 2019

HR professionals in enhancing their role and working effectively with other key departments to mitigate against the insider threat.

This report is designed to create a framework to facilitate this meeting and further investigation. It examines current practice found in a wide variety of organizations, including nuclear transport, operators, regulators, labs and educational facilities.

The findings of this report and any subsequent outcomes will be applicable to but not limited to those working in:

- Nuclear power-related facilities, including nuclear power plants, nuclear fuel cycle and waste management facilities;
- Nuclear research facilities;
- The transportation of nuclear or radioactive material;
- Radiation protection activities; and,
- Other activities affecting nuclear facilities and entities involved in the nuclear industry (such as R&D organizations, suppliers, contractors, technical support organizations and government).

Definition of Security Sensitive Positions

For the purposes of this report, security sensitive positions are defined as those where a breach of trust, for whatever reason, could result in a malicious act that could cause harm to people, damage to property or harm to the environment.

These positions could include any job tasks that allow:

- direct access to radioactive, biological or biochemical substances (materials of concern);
- unrestricted access to any area which could allow access to materials of concern, or access to confidential or restricted information;
- access to confidential, critical and/or secured data (including but not limited to sensitive security, business, financial or corporate information or personnel data);
- the authority to commit financial resources, and/or access to and control over those resources; and,
- positions that require a licence for their execution (e.g., reactor operators) or those designated by regulatory requirements.

Definition of Insider

This report uses the IAEA's definition of insider: "an individual with authorized access to associated facilities or associated activities or to sensitive information or sensitive information assets, who could commit, or facilitate the commission of criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security[2]".

Human Resource Management and the Mitigation of Insider Threats

---

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

Due to its unique nature, the nuclear industry requires a highly trained and competent workforce. In order to ensure that this workforce develops and maintains the correct set of knowledge, skills, attitudes and behaviours necessary to perform the assigned tasks, a set of human resource processes is needed. These processes are collectively referred to as 'human resource management' or HRM. As defined by the IAEA, HRM includes several interacting elements, illustrated below[3]:
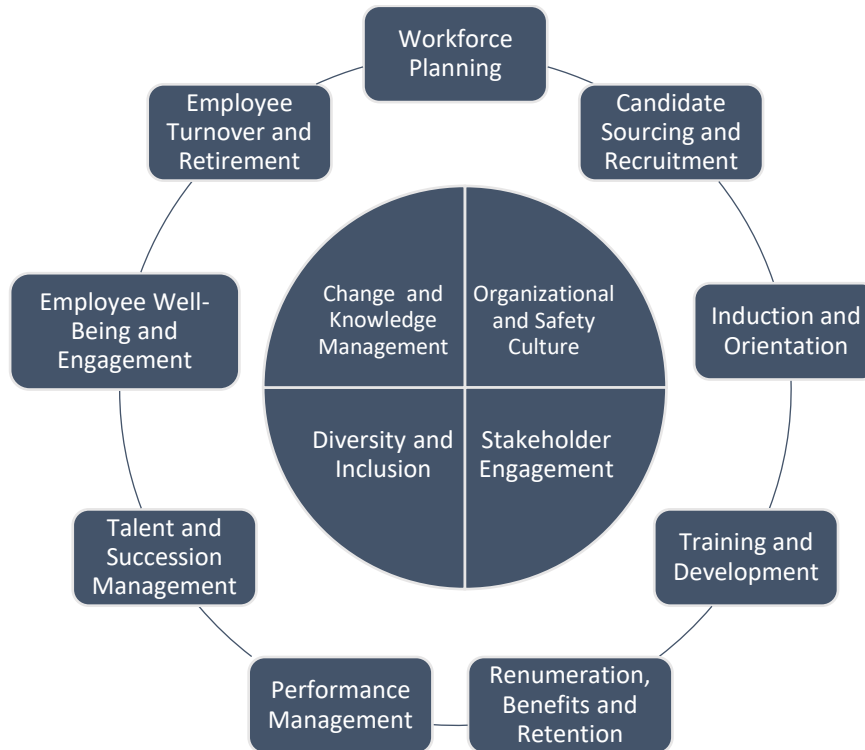
The processes on the outer circle refer to the management of individuals within nuclear organizations, while those in the middle relate to the management of overall organizational aspects.

The management of individuals begins with workforce planning to ensure that the organization has the right number of people with the right set of skills and attitudes at the right time. Based on the outcomes of this analysis, each organization will recruit, induct and train its workforce in order to ensure that the organization functions in a safe, secure and effective manner. This must include appropriate ongoing education and training on individual security matters and the responsibilities of the individuals to the overall organizational security, which the HR department is well placed to ensure reaches all employees. Additionally, the organization must consider mechanisms to retain and manage the talent and succession of its workforce, as well as consider staff well-being and employee turnover. These processes help ensure that an organization's workforce is both competent and managed in a manner that recognizes the value of the individual employee's contribution.

---

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Managing Human Resources in the Field of Nuclear Energy, NG.G.2-1 (Rev. 1), Working Paper, May 2020.

Similarly, processes are needed to support the overall health and development of the organization. These include the development of programs to support knowledge management, organizational, safety and security culture, diversity and inclusion, and stakeholder engagement. Working together, these individual and collective processes will support the performance of an organization and will help foster a culture within the organization that places value on safety and security.

In addition to supporting HRM, the HR department is well positioned to document any abnormal staff behaviour as it is frequently the first point of contact for any employee with personnel-related issues within the organization, whether these issues are their own or a report of a colleague who may be behaving differently.

The Human Resources Department and Underlying Organizational Structure

In many nuclear organizations, the HR function is largely sourced internally, though some organizations outsource various aspects of HR, including screening and vetting. Where HR is sourced internally, the HR department should be considered a trusted and strategic partner of the senior management team. In some organizations, a single individual is designated as the organizational lead on insider threat issues, with ownership for mitigating insider threat and providing knowledge and training across the departments. Where this is the case, HR should be considered a vital part of their wider interdisciplinary team.

HR professionals should possess an ideal interpersonal skill set that allows them to effectively monitor the workforce and the critical pathways to insider threat, which include: personal predisposition; stressors (personal, professional, financial); concerning behaviours; problematic organizational responses (including lack of response); precursors; and hostile acts.

Based on an initial analysis, the key enablers that support the HR department to effectively work to counter insider threat include:

- sufficient staffing resources and funding;
- appropriate training and competencies within the HR team;
- an organizational position which allows them to work effectively across the organization together with senior management;
- recognition that the staff of an organization is a 'front line' for reporting any possible insider threats;
- appropriate systems and technology to support the HR business functions of the organization; and,
- a multidisciplinary team that is able to conduct job task analysis and role-based risk assessment.

One impediment to the creation of an effective insider threat mitigation programme is the siloed structure within many nuclear organizations. This can compromise the effectiveness of programs designed to mitigate insider threats, such as behavioural observation/fitness for duty programmes and the creation of an overall security culture. Facilitating a closer working relationship between HR and other line management functions will allow for the creation and implementation of an integrated and cross-cutting strategy for identifying security sensitive positions and then ensuring that they are appropriately staffed. Closer alignment between HR and the other relevant departments can also simplify workstreams and prevent duplication of work, which can contribute to efficient business practices. This is consistent with

the IAEA's recommended use of integrated management systems that is recognized as a good practice within the nuclear industry.

Senior management buy-in is vital in framing the HR department as an important component of insider threat management programmes, and the HR department should be seen as a strategic partner and take on a transformational rather than transactional role. This includes the requirement not only for representation at relevant meetings but also the provision of adequate training and funding for the HR team to do their job. In addition to management, other stakeholders who should be working closely with HR include:

- Legal;
- Security, including cyber security;
- Fitness for duty/human reliability; and,
- Medical department, including mental health professionals.

In the example of more matrixed organizations, such as national laboratories, this integration is facilitated by adopting a 'business partners' model, so that HR is fully integrated within each team and is best placed to create strong reporting streams. This approach also allows HR to more effectively detect any behavioural anomalies in its workforce, which could indicate a potential insider threat.

Observations and Good Practices

Based on discussions with several countries, it is clear that there is a wide diversity in the level of engagement of the HR department in the mitigation of insider threats. In most countries, positions that have a direct bearing on security require formal authorization, however the methods and practices for authorization vary greatly. In some countries, the regulatory body grants the authorization for positions such as nuclear facility operators, while in others, the operating organization has the responsibility for granting authorization for various nuclear facility personnel. In both models, it is considered a good practice to ensure that the HR team is provided with ongoing security education and awareness training to enable them to identify any red flags which they may come across during their duties.

In general, country-specific regulatory guidance provides the basis for nuclear organizations to conduct specific job-task analyses to determine the knowledge, competence and attitudes that are required for specific roles and tasks. Depending on the safety or security significance of the roles and tasks, processes are established to screen potential candidates. In some cases, this process may include psychometric testing in addition to drug/alcohol testing and criminal background and financial checks. Some organizations use external consultants to support the employee screening process, while others rely on an internal security department or an external national security agency.

The level of involvement of HR varies widely between organizations. Where fully utilised in insider threat mitigation, HR can be used to support the function of ongoing oversight and timely review of security sensitive positions. In most organizations, for example, security clearance privileges are based on continuous evaluations and any out-of-the-ordinary event or behaviour triggers re-evaluation. HR are often on the front line for receiving reports, and must be involved in creating this baseline to allow for earlier detection of deviations, as can be seen in the diagram below:

Clearances and management of change
HR should ensure that the evolving workforce is properly monitored and that appropriate role-based access controls are kept up to date

Job Task Analysis
HR should understand the different competence requirements and security significance of the job positions

Safe reporting environments
HR need to ensure a 'safe space' for reporting, and ensure that concerns are appropriately addresses and where necessary referred to other departments

Continuous monitoring and oversight

Culture and behavioural awareness
HR should have a baseline understanding of the security culture and behavioural trends of the organisation

Performance management
HR must be skilled in creating a baseline of performance and acting quickly upon any red flags

Recruitment, hiring and succession planning
HR should be competent in understanding personal predispositions and detecting red flags

The individual personal predispositions of the managers within an organization play a crucial role in determining the organizational culture. Accordingly, a clear HRM strategy is needed to ensure recruitment, hiring and talent identification practices support the desired leadership characteristics to align with the organization's cultural objectives. In turn, recruiting for leaders on the basis of behavioural fit in addition to technical competence leads to better initial inputs and less necessity for interventionist approaches to organizational culture from the HR or security functions at a later stage.

In addition to the critical areas where HR may support insider threat mitigation, it was also recognized that specific HRM activities are carried out by the HR department that not only support the development of a competent and suitable workforce but also contribute to the development of an organizational culture that promotes safety and security. These relevant activities are listed in the following table:

Elements of HRM	Relevant HRM Activities	Contribution to Organizational Culture
Workforce Planning	- Analysis of workforce needs for the organization. - Conduct job task analysis to recognize security sensitive job positions. - Security risk assessment of personnel to prioritise insider risks to an organization, identify appropriate countermeasures and allocates resources in a way that	- Understanding of the competence (knowledge, skills, attitudes) requirements for each job position. - Development of relationship between HR processes and screening/vetting processes. - Awareness of security sensitive job positions. - Awareness of regulatory requirements.

	is cost effective and commensurate with the level of risk. • Support security/access authorization department with development of screening/vetting process, as requested.	
Candidate Sourcing and Recruitment	• Develop recruitment strategies to identify candidates that are suitable for defined job positions. • Participate in the interview process for potential candidates to support assessment of suitability for the job position. • Once candidates are identified, initiate the clearance/vetting process according to established procedures. • Gather feedback on the recruitment process.	• Understanding of the suitability requirements for each job position, including security sensitive positions. • Development of initial relationship between HR and candidates through the interview process. • Awareness of the screening/vetting process to support effective communication with candidates regarding the hiring process. • Identification of recruitment strategies that deliver more appropriate candidates.
Induction and Orientation	• Provide new hires with general access training. • Provide training on fitness for duty programs and insider threat awareness. • Provide departmental specific induction programs.	• Development of relationship between HR and fitness for duty programs. • Establishment of HR as a "safe space" to receive employee concerns or questions. • Opportunity to create initial expectations of the organizational culture.
Training and Development	• Line managers and HR continuously review the competencies required for each job position to ensure the availability of adequate and appropriate training. • Leadership development programs are in place for senior management. •	• Training ensures that all individuals (including the HR team) have the necessary technical skills and competencies. • Training programs can serve to highlight the importance of teamwork for staff. • The use of leadership development programs will help guide the overall culture of the organization.
Remuneration, Benefits and Retention	• Develop reward strategies and benefits packages that attract, retain and motivate staff. • Ensure staff are fairly compensated according to their job position and take into account overtime compensation.	• A properly rewarded staff will be motivated to help the organization meet its objectives. • The availability of health insurance ensures access to medical and mental health professionals when needed and promotes well-being.

| Performance Management	• Conduct performance management appraisal meetings with staff. • Establish coaching or mentoring programs between staff at different levels within the organization.	• Provides an opportunity to evaluate individual performance and reinforce the organizational culture. • Specific key performance indicators may be used to evaluate the individual's contribution to supporting a safety and security culture. • Mentoring programs help promote the organizational culture between staff.
Talent and Succession Management	• Develop programs to identify and encourage the development of staff with management potential. • Create knowledge management programs to capture or share specialized knowledge or skills.	• Leaders that are developed from within the organization will likely understand the culture of the organization better. • Knowledge management programs should be developed as part of an organization's management system.
Employee Well-Being and Engagement	• Develop mechanisms to receive staff feedback. • Develop strategies to support a safe, healthy and respectful working environment. • Establish arrangements to support staff in certain circumstances (flexible hours, parental leave, career breaks, etc.)	• Any feedback received can contribute to the continuous improvement of the organizational culture. • Staff that feel that they work in a safe, healthy and respectful environmental will likely reflect these values back. • Arrangements to support staff in certain circumstances will keep them engaged in the organization.
Employee Turnover and Retirement	• Conduct exit interviews for staff leavening the organization.	• Creates a better understanding of why individuals are leaving an organization, especially those that were employed for only a short time.

Finally, it was found that the availability of specific competencies within the HR department could support the mitigation of insider threats. These include:

- A clear understanding of the security sensitive nature of working in a nuclear organization to facilitate their ability to select individuals with correct attitudes and values;
- The ability to form and maintain a close working relationship with relevant departments (e.g., safety, security, medical officers, fitness for duty), line managers and senior management;
- Competencies in job task analysis and assessment practices;

- The ability to consider the security implications of behaviours and to refer any concerns to the proper department;
- The ability to support an organization's insider threat management programme from the outset of the employee lifecycle through training in interview techniques and red flag detection;
- An awareness that appropriate education and experience are not sufficient indicators to ensure that an individual is the right fit for a security sensitive position – personal predispositions must be considered when assessing candidates for security sensitive positions;
- Competencies in mental health and psychology[4] or access to mental health professionals;
- Competencies in organizational design and structure, which can help facilitate sustainable insider threat mitigation programmes;
- Root cause analysis training, which can help allow institutional knowledge to become embedded; and,
- An holistic approach to employee well-being and management that allows for a strong and supportive relationship, allowing for more effective insider threat mitigation.

Conclusions and Next Steps

Based on this initial analysis, it is clear that the HR department and its respective HRM activities support both the mitigation of insider threat as well as the development of an organizational culture that values nuclear safety and security. The HR department is well placed to intervene in the critical pathways to insider threat, creating 'choke points' to prevent an employee who is experiencing difficulties from progressing through to the 'hostile act' stage. This can be seen in the figure below:
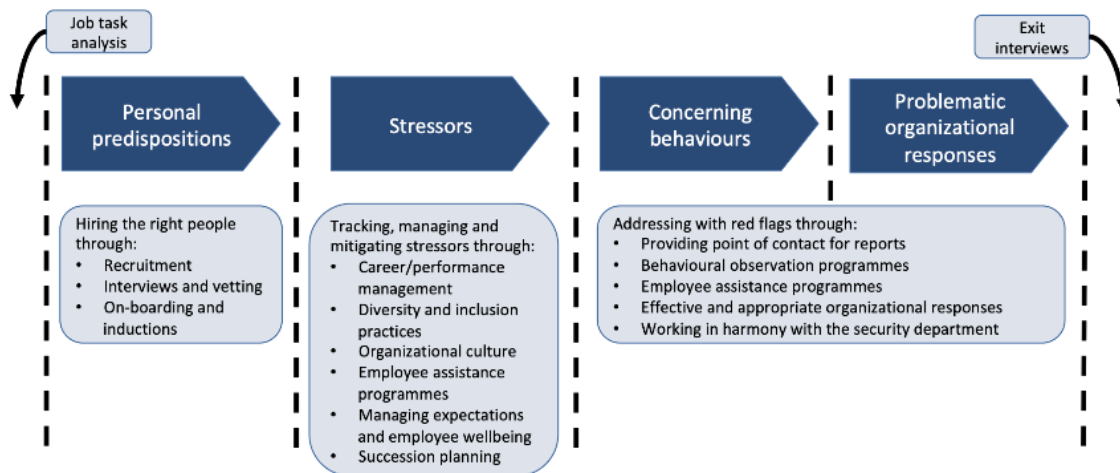
Given the variety of approaches to integrating HR into the process of identifying security sensitive positions, as well as subsequent screening and fitness for duty programs, and the varying levels of involvement, it would be beneficial to bring together a diverse group of countries and organizations to share their experiences. This would provide an opportunity to build a consensus around the findings collected in this paper and develop good practice guidelines and methodologies to help organizations to facilitate the enhanced involvement of human resource professionals in insider threat mitigation.

---

[4] CDSE webinar on Human Resources and Insider Threat; https://www.cdse.edu/catalog/webinars/insider-threat/human-resources.html