Addressing Insider Threats with Resilience and Fortitude

Adv. Karen Pillay, Eskom Group Security;
Ms. Karen Kaldenbach, Oak Ridge National Laboratory

Abstract

Nuclear and most other industries faced many challenges in 2020. As many organisations shifted to new ways of working in a remote environment or at least with limited personal interaction between staff, it became a challenge to not only maintain security and safety protocols but also to provide due diligence to trustworthiness and reliability programs. This year was a reminder that part of ensuring the safety and security of nuclear facilities and staff includes resilience in insider threat mitigation efforts, protecting against those who may intentionally or unintentionally interject points of failure into facilities.

In 2020, the Koeberg Nuclear Power Station (KNPS) operated by Eskom near Cape Town, South Africa, sought opportunities to maintain optimal productivity. Eskom took advantage of reduced power needs when many businesses closed and expedited its maintenance schedule. This requires great rigor to enhance maintenance while supporting necessary pandemic protocols and maintaining required security and safety measures.

This paper will address the processes applied by Eskom to ensure insider threats were not introduced to KNPS during increased maintenance activities, as well as lessons learned from improving resilience in the fitness-for-duty program and overall insider threat mitigation program at Eskom.

1. Introduction

The COVID-19 pandemic brought with it many nerve-wracking challenges for individuals and organisations. Governments were also confronted with enormous pressure to confront the risks and implement controls needed to prevent the spread of the virus, and to accomplish this, they had to implement policies to address the containment of the infections and the pandemic. Due consideration also had to be given to the social, psychological, technological, and economic pressures that plagued society. The prominence of psychological and social pressures definitely manifested and were brought on by the pandemic due to the prolonged lockdowns and isolation of individuals. These pressures began to directly and indirectly affect individuals world-wide. The impact of the pandemic was and is still overwhelming. To this day, we are continually exposed to a mutation of the virus and various waves that cause infections to reach unprecedented levels. Organisations are also forced to implement controls and measures to contain the virus and to create safe workplaces. At nuclear facilities, the importance of human resources, physical restrictions, social distancing, rotational and remote working, daily screening, and testing were implemented to not only curb the spread of the virus but also, and more importantly, to ensure safety and security of the facility. Throughout these pressures—and coupled by government policy changes and changes in organisations—there should not be any degree of complacency.

2. Insider effect

The term *insider*[1] is used to describe an adversary with authorised access to a nuclear facility, a transport operation, or sensitive information. People within an organization (employees, contractors, regulators, business partners, etc.) can pose a risk to operations, security, and processes in the organisation because they may have intimate knowledge of the organization and security processes and systems that may allow them to bypass the system. KNPS is Eskom's and South Africa's only nuclear plant, so extra care and precautions are always taken to ensure that the physical protective systems are effective and that all safeguards and safety measures render the necessary mitigation and control of risks.

Insider threats presented by employees and contractors are challenging because they have knowledge of the security processes, systems, and those with access rights to critical systems that may allow them to bypass the system. Outsider collusion is also problematic. Both categories of individuals can react on a single impulse or in a premeditated manner. Most known material theft incidents involved insiders because insiders

- have access to areas of the facility;
- exercise authority over other personnel;
- have technical knowledge, skills, and experience; and
- have access to systems, equipment, and tools.

Figures 1 and 2 clearly articulate the psychosocial effects caused by the COVID pandemic. No doubt the high reliance on medical assistance or use of substances could have increased as a result of the pandemic. These factors lend insiders vulnerable and susceptible to risks and posing risks to site security and operations.

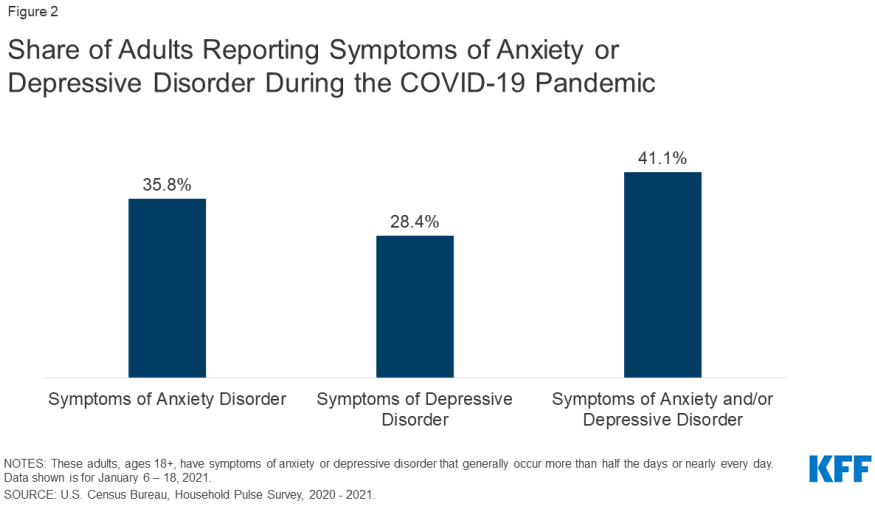

Figure 1: Percentage of adults that reported anxiety and depressive disorders. Reproduced from N. Panchal et al. "The Implications of COVID-19 for Mental Health and Substance Abuse." Kaiser Family Foundation. February 10, 2021.

[1] IAEA Nuclear Security Series No. 8-G (Rev. 1) Implementing Guide—Preventative and Protective measures against Insider Threats. International Atomic Energy Agency, Vienna, Austria.

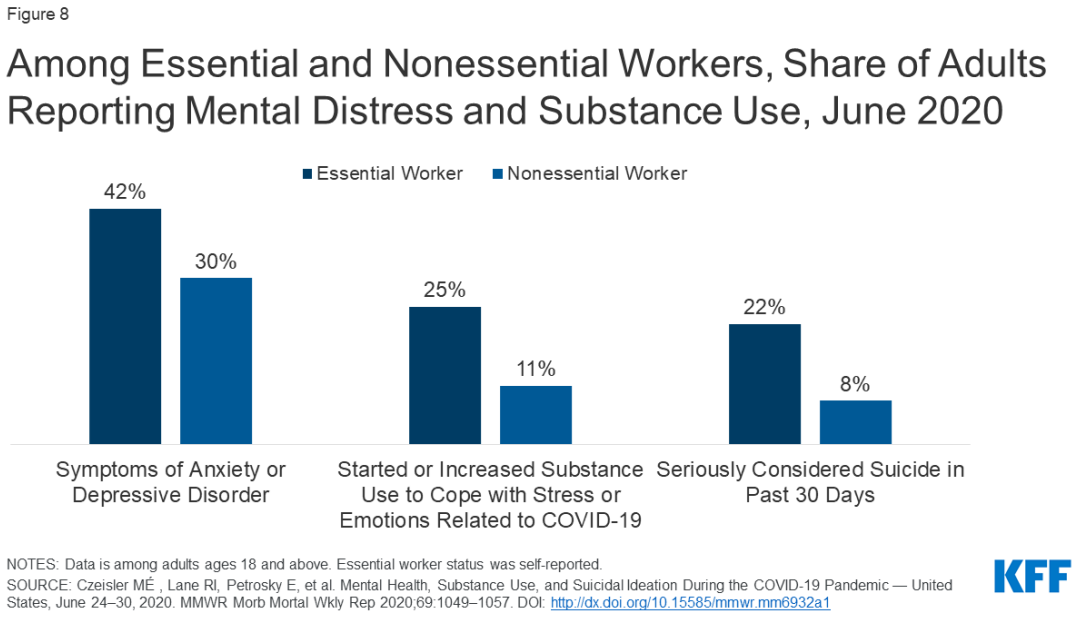

Figure 2: Percentage reporting of mental distress and substance abuse between essential and nonessential workers. Reproduced from N. Panchal et al. "The Implications of COVID-19 for Mental Health and Substance Abuse." Kaiser Family Foundation. February 10, 2021.

3. South African Regulatory Framework applicable to Nuclear facilities

In South Africa, there is legislation that compels nuclear facilities, such as Koeberg, to manage their security and processes. Koeberg is a site of national importance and is integral to the electricity supply network.

The security regulatory requirements for Koeberg include the following legislations:

- The National Nuclear Regulator Act[2], (Act No. 47 of 1999)
- National Key Points Act[3] (Act No. 102 of 1980)
- Nuclear Energy Act, 1999[4] (Act No. 46 of 1999)
- South African Police Services (SAPS) Act, 1995 [5] (Act No. 68 of 1995)
- Seashore Act, 1935 [6](Act No. 21 of 1935) (amended by Act No. 51 of 1997)
- Civil Aviation Act, 2009[7] (Act No. 13 of 2009) - FAR 36
- Integrated Coastal Management Act[8], 2008 (Act No. 24 of 2008)

[2] Act 47 of 1999
[3] Act 102 of 1980
[4] Act 46 of 1999
[5] Act 68 of 1995
[6] Act 21 of 1935 amended by Act 51 of 1997
[7] Act 13 of 2009
[8] Act 24 of 2008

- National Strategic Intelligence Act9, 1994 (Act No. 39 of 1994)
- Protection of Constitutional Democracy against Terrorism and Related Activities Act, 200410 (Act No. 33 of 2004)
- Firearms Control Act11, (Act 60 of 2000) [12]; and
- Private Security Industry Regulation (PSIR) Act12, (Act No. 56 of 2001)

4. Eskom and Koeberg Nuclear Security Policy

A robust nuclear security policy governs the rules and processes at the Koeberg site to ensure that high degrees of performance, compliance, and enforcement are maintained. Eskom's intent for security management and compliance is entrenched in Eskom's Security Management Policy, which has the core objective of protecting the organisation's assets (people, information, infrastructure, systems, and processes).

In addition to Eskom's Security Management Policy, Koeberg shall embed the principles at the site level and issue its own nuclear security policy statement that includes the following:

- Establishing and implementing the nuclear security policy at all levels, including senior management
- Ensuring that the security policy principles support the organization's business plan to create value for all stakeholders and to provide security for its personnel, property, assets, and information
- Ensuring compliance with national and international legal processes
- Appointing different stakeholders to ensure adequate nuclear security measures are implemented
- Ensuring that security personnel receive accredited physical protection training
- Ensuring the interface and synergy between security and safety features in preventing and responding to sabotage and theft of radioactive material, as well as during emergency circumstances
- Ensuring that all personnel are fully aware of their roles in the implementation of the policy

a. Koeberg Nuclear Security Code of Conduct

KNPS has a defined security code of conduct upon which all individuals are trained when they join the company or provide a service (i.e., subcontractors). The code of conduct states

> Our success depends on each of us living up to the Eskom values and the following nuclear security standards. Hence, we commit that we shall:

[9] Act 39 of 1994
[10] Act 33 of 2004
[11] Act 60 of 2000
[12] Act 56 of 2001

- Maintain the highest standard of security operations and reliability for our people, the customers, and our communities.
- Ensure safety first and in so doing shall maintain an effective nuclear security operations and culture.
- Excel beyond compliance and exceed standards of performance daily.
- Respect our colleagues, superiors, and customers.
- Perform with integrity and shall take accountability for our actions.
- Innovate and promote continual improvements in our daily operations.
- Treat and respond to every single threat as a real threat.

b. Importance of Nuclear Security Culture

All staff receive training on the importance of nuclear security culture as the backbone to maintaining not only effective security within the site, but also contributing to a good safety culture. Premises of the nuclear security culture program include:

- Integrate security into the operating unit and daily operations.
- Invest in the security workforce.
- Revitalize/refurbish and maintain the site security infrastructure.
- Promote innovation and efficiency in nuclear security.

c. Koeberg Nuclear Observation Programme

As part of the fitness-for-duty program at KNPS, a nuclear observation program is an essential element of maintaining effective safety and security. This program states that, "Security areas and processes to be part of Plant Observation Plan."

d. Leadership Behaviour Observation Cards

All KNPS managers and those in any leadership role submit behaviour observation cards to demonstrate effective attention and observation in the course of doing their daily assignments and remaining cognizant of the activities of their staff members. The process requires that security be included for observation purposes

e. Marketing Calendar, Marketing Material, and Monthly Themes (aligned to IAEA Series 7)

KNPS has determined that by creating marketing material and using the calendar to focus on specific safety and security themes, it can increase awareness and helps staff incorporate security into their daily activities, improving security culture and minimizing the likelihood of insider threats. KNPS has the following monthly themes this year:

- January Questioning unusual behaviour
- February My attitude to nuclear security

- March Information security
- April Access control—importance and breach of procedures
- May Searching and seizure of prohibited items
- June Testing for alcohol and substance abuse
- July Following the rules for facility security
- August Reporting incidents and unusual behaviour
- September Secure your assets
- October Staff trustworthiness
- November Handling sensitive/classified information
- December Fitness for duty programme

Figure 3: Eskom's security culture maintenance and continual improvement pillars.

5. Use of the Threat Risk Assessment and Risk-Adjusted Strategy

The threat risk assessment (TRA) is one of the tools used by Eskom security management to determine the threat or risk against Eskom people, assets, and information and to develop protection measures to minimize or neutralize threats or risks. The assessment is updated on a regular basis or whenever the security threat changes. The objective of the TRA is to identify and evaluate the critical assets and infrastructure at Koeberg.

The definition of a threat is based on the potential types of adversaries. Generally, adversaries are categorized into three broad groups: outsiders (terrorists, criminals, violent activists, etc.); insiders; and outsiders colluding with insiders. These entities operate under the flag of the Coalition Against Nuclear Energy South Africa with affiliations to Greenpeace and Earth Life Africa.

a. Findings of the Koeberg Security Threat Assessment

Priority	Threat	Probability	Impact	Mitigating Measure
1.	Loss of life caused by assault	Low	Severe	Installation of proper public exclusion boundary
2.	Small aircraft crashes on site	Low	Minor	Declared no fly zone in terms of FAR-36
3.	Runaway veldt fires	Low	Minor	Use fire breaks/fire break roads
4.	Protest actions	High	Medium	Demarcated area for protest actions
5.	Illegal occupation of Eskom land	Low	Minor	Perimeter security fence and access gates are installed
6.	Malicious damage to Eskom equipment and property	Low	Minor	Access is controlled and intrusion detection system installed
7.	Theft of Eskom equipment and vehicles for financial gain	Low	Minor	• Access is controlled • Intrusion detection systems and security lighting installed on-site • Security patrols
8.	Criminal acts caused by insiders and outsiders	Low	Minor	Security clearance and vetting of personnel
9.	Kidnapping/hostage situations on- or off-site to Eskom key employees and contractors	Medium	Medium	Security awareness programmes are conducted to educate Eskom employees, visitors, and contractors
10	Unauthorised drone usage	Medium	Medium	Implement counter drone detection technology

b. The Eskom Risk Adjusted Strategy for the Pandemic

To ensure all safety and security risks were properly identified and managed during the pandemic, several deliberations occurred across the Eskom businesses, including the Koeberg Nuclear Plant. A key

development for Eskom was the formulation of the risk-adjusted strategy that was to be used to manage the outbreak of the pandemic, the pandemic, and epidemic disasters, as an organisational and national priority. Serious scenario and disaster planning events were undertaken and forced the business areas to remain in constant risk assessment mode and response, while learning from others. The World Health Organisation directives were also relied upon to inform ley business operations while focusing on the security of supply of electricity and safe operations of all national Eskom sites.

Managers at all levels and businesses across the organisation were assigned specific responsibilities to execute the organisational risk adjusted strategy and response plan, with a key focus on the following:

- **Implementation of Alert Levels nationally**—All government imposed alert levels were consistently applied across Eskom, and, where the Koeberg facility was concerned, higher levels of measures were implemented which were on occasion higher than the national level. This was done purely to manage and contain spread of infections at sites.
- **Institutional arrangements**—The Eskom Pandemic Disaster Management Plan was focused on implementing wide spectrum preventative measures and incident command across the various tactical command structures throughout the business. A constant situational awareness capability was established and implemented on a single digital platform the organization can access and use in decision-making.
- **Protecting the security workforce**—The security workforce was tasked with screening and testing controls in addition to their daily security functions. This increased their risk exposure, necessitating the effective use of additional PPE and frequent testing and monitoring. A nifty tool to assist was remote temperature monitoring cameras. Sanitization protocols were increased for tools, equipment and objects with which security personnel came in contact.
- **Staff authorisation, testing, and movements**—Only authorised staff and personnel with permit-holders are allowed access to sites provided COVID and substance testing is conducted. No casual visits are permitted at site.
- **100% mass testing**—The access authorization is only granted when an employee or contractor completes the required testing without exception and meets the testing standards. Any employee who fails the tests or refuses to be tested is refused access to site and may be subjected to disciplinary action.
- **Use of sanitization and PPE**—Serious protocols are in place to ensure adherence to regulatory and site-based measures and health protocols.
- **Use of sterile quarantine facilities**—Critical facilities were earmarked and reserved during lockdown conditions to ensure that exposure of critical personnel or contractors to infections was reduced.
- **Deferment of non-critical maintenance activities**—Management was proactive in identifying maintenance activities that could be deferred to a later date to minimize exposure.
- **Revised security measures**—All sites including the nuclear power station were escalated to heightened alert levels because most employees were working remotely, and areas of the sites needed to be kept sterile and secure. Security processes such as access control, incident

monitoring and response, site patrols, temperature screening, and testing were increased, and new technologies and equipment was introduced to assist the security workforce to proactively manage security, compliance, and performance without compromising safety and security standards.

- **Staff and contractor screening and vetting**—All security screening and vetting protocols remained intact, and all attempts were made to randomly select and screen individuals.
- **Remote/virtual workspaces**—The rapid implementation of remote/virtual workspaces was implemented across the business. This necessitated that secure networks were established to ensure continued employee productivity and attendance. All related threats and risks were identified, and new ways of working and new workplace strategies were developed and implemented. These measures are continually being reviewed for improvement. Various business processes were virtualized (e.g., procurement, auditing, investigations) as far as practically possible.
- **Materials and inventory management**—A thorough process was implemented to ensure the management and control of critical equipment, spares, and related assets including nuclear material at KNPS. The management and control of nuclear material is constantly monitored, and the integrity of processes are managed through audits and surprise inspections, to ensure that integrity is maintained throughout the processes and to prevent theft and loss of nuclear materials.
- **Staff classification and categorization**—The focus was to make the workplace the safest, and to accomplish this, only critical staff were permitted on-site. Quarantine and isolation facilities were earmarked on-site and prepared for use to ensure sterile and infection-free conditions for staff and contractors. The 14-day self-quarantine rule was implemented for spare shifts to ensure availability of resources, as they were confined to their residences during this period. A 14-day quarantine period was also applied for contractors that travelled from abroad and access authorization was granted upon completion of testing with negative infection and prohibited substance results. No exceptions were made, and strict compliance was enforced at all times and continues to be applied at site.
- **Awareness campaigns**—Constant communications and awareness are conducted for all security threat and risk issues as scheduled or immediately when there are indications of changes in the risk profile.
- **Peer-to-peer engagements and benchmarking**—Peer reviews and engagements are useful to test and consult on common issues and topics that are applicable to the insider threat and mitigation strategies. It is also stimulating to share successes, failures, and lessons learned.

6. Conclusion

The pandemic we are experiencing is unprecedented and requires a high degree of resilience and responsiveness to the changing conditions and circumstances. The nuclear industry is equally confronted with risks, issues, and challenges given the local and global changes. Increasing the remote work footprint and expanding the services and access to information increases demand on management and individuals to adopt and comply with stricter controls and mitigation measures.

The success of 100% mass testing no test–no entry rule as a measure certainly assisted Koeberg management with containing infections on-site and protected critical resources and the workforce, especially during the outage. Figure 4 shows how testing helped to flatten the curve.

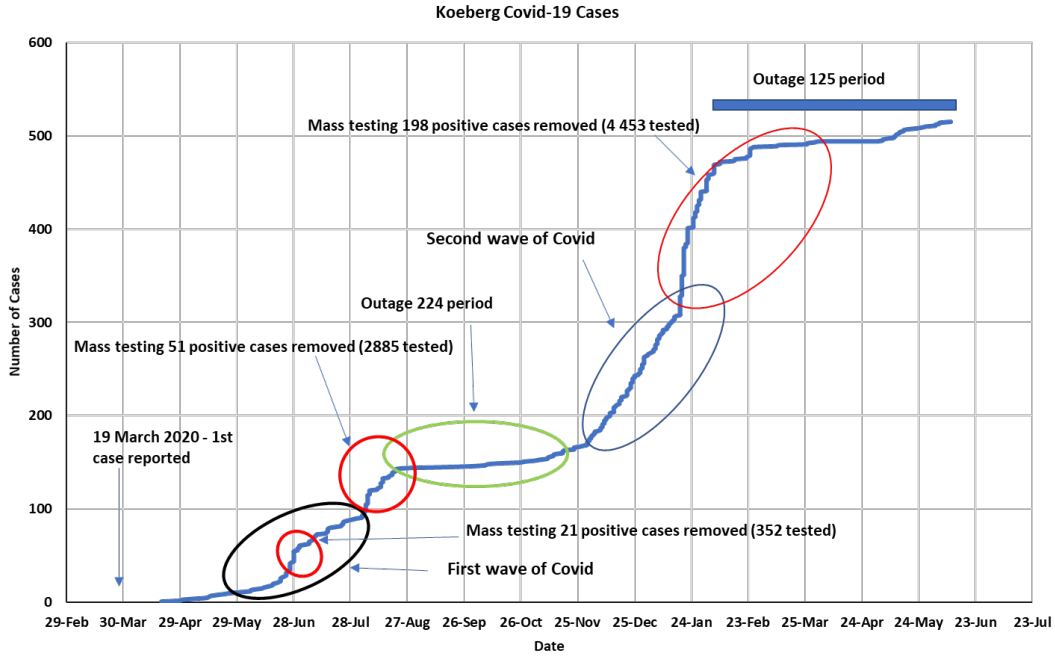

Figure 4: Mass testing results and trends at KNPS from inception of the pandemic.

In addition, the effective use of systems and technology also promote safety and security. The insider threats must be constantly monitored to detect vulnerabilities and blind spots. Sharing lessons can be a valuable exercise. Scenario planning and stress testing thereof is always useful to assess the effectiveness of measures and programmes. Working within the ambits of legislation is peremptory but what is more crucial is to maintain a balance between operations, safety and security of individuals and operations. Prevention is always better than cure, and the insider will always be the weakest link when complacency sets in.