NEMZETBIZTONSÁGI SZEMLE
11. évfolyam (2023) 1. szám 49–61. • DOI: 10.32561/nsz.2023.1.4

Ákos Bunyitai[1]

Insider Threat Mitigation in High Security Facilities

The biggest challenge for the security in high security facilities is the insider threat, humans as the weakest link of the system. The insider is an invisible enemy of the security, because it has unique capabilities. Although perfect security cannot exist, the aim of the present study – besides showing the threat represented by insider offenders – is to introduce the measures for risk mitigation.

Keywords: *security, protection, prevention*

The story of the Trojan Horse used during the Trojan War is well known. The Trojans pulled into the protected city of Troy a huge wooden horse, with Greek soldiers inside. At night the Greek force crept out from the horse and opened the gates of the city under siege for the rest of their army. The Greek army entered the city of Troy and destroyed it. Success was due to the assistance given to the external part of the Greek army from inside the well protected city walls, by the soldiers from the wooden horse. From the time of Homer's ancient epic poem, Iliad, a "Trojan Horse" means any trick or stratagem that makes someone "invite" a foe into a securely protected area who then attacks from the inside. The problem of the possible hostile element in any secured area is still relevant. As Matthew Bunn and Scott D. Sagan wrote: "Insider threats are perhaps the biggest and most difficult part of the security challenge."[2]

Who are the 'insiders'?

To put it simply, an insider is an internal adversary, who has capabilities and opportunities to perform malicious actions; therefore, an insider is a security threat. Let us see the most relevant/important definitions used by the supporting guides of the International Atomic Energy Agency (hereinafter: IAEA). The IAEA was among the first to recognise

[1] MSc, Security Engineer, Student of Óbuda University Blasting Technology Engineer Postgraduate Specialist Training, e-mail: bunyitai.akos@gmail.com

[2] Bunn–Sagan 2016: 171.

the threat of an insider and published its definitions and suggestions for the mitigation of possible harms from the point of view of nuclear security:

Adversary

An adversary is any individual performing or attempting to perform a malicious act. They may be an insider or an outsider.[3]

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."[4]

Threat

"A likely cause of harm to people, damage to property or harm to the environment by an individual or individuals with the motivation, intention, and capability to commit a malicious act."[5]

Malicious act

"An act or attempt of unauthorized removal or sabotage."

The illegal, malicious act that may cause any harm or damage may vary by every facility. It depends on the local legal background, the profile of the company, and many other factors. For example, the main goal for the physical protection system in nuclear facilities is to protect radioactive material from unauthorised removal and also to protect nuclear facilities from sabotage and – in case of sabotage – minimising the radiological consequences.[6]

[3] IAEA 2020.
[4] IAEA 2013: 12.
[5] IAEA 2008: 1.
[6] IAEA 2011: 52.

Who can be an insider?

In order to understand the scale of the threat, let us clarify the persons, who can become insiders. It can be anybody who has permission to enter the site and/or authorised access to the systems of the facility, thus in particular, but not exclusively:

- officials of the management of the facility
- employees of the facility
- security personnel, guards
- system administrators of the IT system
- external contractors, partners
- maintenance personnel
- official persons
- employees of public utilities (electricity, gas, water, sewer, Internet, waste management)
- vendors, courier
- visitor

Insider types

The division of the insiders by types is largely theoretical, its practical significance is negligible. In the majority of cases, the identity of the insider is revealed only once the illegal act had been committed (before that, they can be considered 'potential' insiders if they are suspected of hostile activities). In the preparation phase, it is difficult to predict how they would act, what is their motivation, whether they would act aggressively. In many cases, their intentionality is also questionable. The following categories are used to review the insiders and to be ready to face the threat. Types of insiders:

1. passive (always non-violent, only provide information)
   - unintentional or unwitting[7]
   - intentional
2. active (always intentional)
   - non-violent insider (perpetrates an act himself/herself or assists others to committing)
   - violent insider (ready to use physical violence against personnel or others)

Possible insider tactics

According to the IAEA's statement, an "insider can pose many different types of threats to a facility".[8] The insider when committing an illegal act, can act alone or in

[7] Unwitting insider: the unwitting insider is unaware of their involvement in the attack.

[8] IAEA 2020.

cooperation with – even in preparation for an external attack – other colleagues or a group from outside the facility. Their action can be quick (e.g. cutting a hole on the fence) or even protracted in time (e.g. protracted theft, smuggling in small amounts of explosives). Some of the actions are very difficult to detect.

1. Possible passive insider tactics
   - transfer of available sensitive information to an external person (regarding the weakness of the security system, the facility and its operation)
   - transfer of own access rights (knowledge-based or physical token)
   - loss of sensitive information
   - testing the security capabilities of the facility
   - other non-violent acts

"The passive insider provides only the information that he or she can readily obtain and divulge without fear of detection."[9] In many cases, the employee unknowingly, unintentionally, accidentally and with good intentions helps the malicious act (e.g. as a victim of social engineering), thus becomes a passive, unwitting insider. He or she can gossip (e.g. CEO's hobby), or transfer useful or even sensitive information (e.g. new security guards), can be inattentive, and forget an access card somewhere, can 'piggybacking'[10] or take any subject avoiding the security control, breaking the security culture, rules and legislative regulation.

2. Possible active insider tactics
   - unauthorised entry (e.g. breaking of locks)
   - testing the security capabilities of the facility
   - disinformation of the security organisation
   - theft (e.g. keys)
   - manipulation of sensitive information
   - falsification of database or blueprint
   - tamper or sabotage of security system
   - sabotage (e.g. by improper handling, damage, explosives)
   - preventing authorised access
   - cyberattack (it can result in physical damage also)
   - neutralisation of security staff or response forces
   - disruption of the normal operation of the facility, jeopardising business continuity
   - other non-violent or violent acts

The real difference between passive and active insiders is how they carry out their activities. An active insider is always an active participant in the plot, risking of being caught. If the insider gives his or her own key to the adversary, he or she is a passive

[9] Sandia National Laboratories 2019.

[10] Piggybacking: when an authorised person opens the door for an unauthorised person to enter.

insider; but if he or she steals or copies his or her colleague's key, he or she becomes an active insider.

An active, non-violent insider uses stealth and deceit, not force, against personnel; while an active, violent insider is ready to use force against personnel. An active insider cannot be an unwitting one, because he or she is always aware that what he or she is doing is helping the attack.

It is noteworthy, that damage can be caused not only by unauthorised access to something, but also by intentional (or unintentional) damage by authorised access and by unauthorised blocking of access as well. Anyone who has logical and/or physical access to something, has a good chance of being able to block it from others (e.g. blocking access to fire water, blocking access to utilities or blocking the doors of the security personnel). Picking a lock and replacing it with your own lock may be a preparatory step for an attack: ensuring that the obstacle is overcome more quickly and less conspicuously during the attack. Both, the passive or active – even violent – insiders may be responsible for testing the security capabilities of the facility (e.g. response time of the guards), even with actions disguised as innocent mistakes.

Motivation

The possible motivation of the insider can help to understand their behaviour and to prevent becoming an insider. The security personnel cannot be sure that the insider's act is rational. An unwitting insider does not have motivation. As stated in the Sandia National Laboratory's publication: "Motivation is an important indicator for both level of malevolence and likelihood of attempt."[11]

Some of the possible motivations:

- financial
- ideological
- coercion
- psychological
- revenge/embarrassment
- ego
- mental stability
- combination of the above

Attributes and advantages

The advantages of insiders is that they are able to: be "invisible" for the security organisation, because no one suspects them; they can explore their options freely and unobtrusively; test the security capabilities without consequences; choose the best time; select the most vulnerable target; may associate with other insiders or outsiders. "Insiders possess at least one of the following attributes that provide

[11] Sandia National Laboratories 2019.

advantages over external adversaries when attempting malicious activities: authorized access, authority, knowledge."[12]

1. An insider may have authorised logical and/or physical access[13] to information, equipment, system, thus in particular, but not exclusively:

- databases
- IT and communication system
- regulations
- protocols and procedures
- plans, even to security plan and contingency plan
- premises, even to office, storage, armoury, server room
- equipment
- tools
- vehicles
- systems, even to security system

In summary: an insider may have authorised access to everything that is factually in use by the company.

2. An insider may have authority when performing his/her duties thus in particular, but not exclusively:

- management of certain systems (e.g. remote system control, shutdown, disconnect)
- managing subordinates (e.g. override internal rules by verbal instruction)

3. An insider may have knowledge and skills in particular, but not exclusively:

- facility-level knowledge
  - location
  - access routes
  - buildings, floor plans
  - utility networks
  - operational information
- organisation-level knowledge
  - management
  - organisation structure
  - position of employees
  - contact details of employees
  - subordinate–superior relationships
  - rules, protocols, procedures, policies
  - personal information (family and friendships, hobby, etc.)
- professional-level knowledge

[12] IAEA 2020

[13] Logical access to virtual, non-material items; physical access to material items (for more information see IAEA 2011; IAEA 2018).

- security-level knowledge
  - detection and delay equipment's type, location, number, guard's location, patrol routes, security protocols
  - vulnerabilities
  - offensive tactics, weapons, martial arts skills, explosives
  - external response force
- external partners, suppliers
  - contracts
  - expected deliveries and dispatches
  - waste collection arrangements
  - mechanics, maintenance

As detailed above, it can be seen that the possibilities for insiders range widely, the circumstances are in their favour. What can the security organisation do? "Quis custodiet ipsos custodes?"[14]

Insider threat mitigation

After the target has been identified, the first step is to specify defensive measures to mitigate insider threat. Understanding preventive and protective measures are the keys to mitigate the insider threat; to detect, to delay and to respond to the malicious act and also to minimise the effects of the adversary act.

1. Preventive measures: "Identifying undesirables behavior or characteristics, which may indicate motivation prior to allowing them access; minimize the opportunities for malicious acts by limiting access, authority and knowledge."

2. "Protective measures: Detect, delay and respond to malicious act."[15]
The key is to reduce the opportunities to perpetrate any malicious act to the lowest possible level with preventive measures, as shown in Figure 1. In case if there is still another insider with opportunity for malicious act, protective measures have to help to detect, delay and respond to minimise the negative consequences of the insider's act. The deterrent factor of the preventive and protective measures is also effective, however, it is hardly measurable.

[14] "Quis custodiet ipsos custodes?" is a Latin phrase from Juvenal's Satire VI meaning: "Who will guard the guards themselves?"

[15] IAEA 2021.

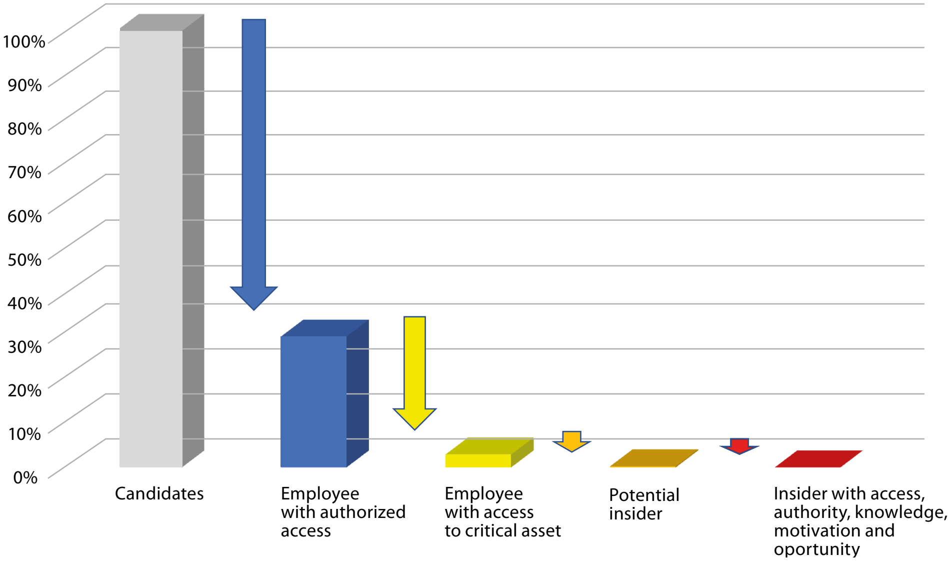

Figure 1: Reduce the opportunities with preventive measures
Source: compiled by the author

3. Main steps and useful tools to mitigate the insider threat
The effective tools to mitigate the insider threat are in the hands of the Management, the Human Resources Management and the Security Department of the facility. These contain preventive and protective elements of corporate policy, partnerships, internal rules, procedures, protocols and security system.

- Prevention of transformation into an insider globally
  At the macro-economic level i.e. at the level of the general regulation, the State sets out the normative legislation and lower level regulatory act which in disfavourable cases may trigger someone to become an insider. On the other hand, good insurance, favourable employment conditions and a good taxation system can avoid the conversion of individuals into insiders.
- Avoid the problem
  It means that inside the company a good recruitment process has to be developed to avoid recruiting people with high security risks. Do not employ someone who is a potential threat!
  The employment of a risky individual is avoidable by:
  - cooperation with authorities, intelligence services and investigating authority
  - cooperation, exchange of information and experience with other high security facilities
  - employing the best possible and reliable staff necessary for the operation of the facility and for the performance of security tasks in-house

  - developing appropriate recruitment requirements for jobs (e.g. security clearance, psychological screening, avoiding persons with dependency or other factors owing to which an individual could be coerced later)
- Prevent the transformation from employee to insider[16]
  The company encourages loyalty by offering favourable conditions to its employees to prevent their dissatisfaction.
  - clear management communication and management reporting to employees on issues that affect everyone (e.g. employee forums, regular meetings)
  - open communication between departments
  - a clear and transparent organisational structure (hierarchies, responsibilities)
  - corporate security culture, security awareness training (entry-level and refresher training, out-of-sequence training if necessary)
  - encouraging questioning behaviour
  - maintaining alertness (e.g. reducing workload, taking rest periods)
  - supporting the integration of new employees (mentorship program)
  - developing a system that encourages employee loyalty, low turnover and employee satisfaction, and retention: a stable and predictable working environment, a career development model, good relations between employees and between management and employees, a high pay and reward system, fringe benefits, positive feedback
  - encouraging less inter- and intra-departmental rivalry and teamwork (e.g. by organising training sessions)
- Reduce the opportunities
  The security organisation reduces the opportunity of malicious act with regulators and controls.
  - introducing a tiered licensing system – sharing of rights – to reduce the likelihood of extortion, coercion, threats and abuse
  - encouraging continuous training, further training and self-training of the security organization (learning new tools, tactics and methods)
  - developing an audited supplier system
  - avoiding an over-regulated environment[17]
  - creating, communicating and enforcing a regulatory environment that is logical, reasonable, transparent, understandable, clear, strict but fair and enforceable, and applies equally to all
  - enforcing compliance where necessary (e.g. through the operation of security system, consistent sanctions for non-compliance and exceptions)
  - keeping the regulations up to date, revising and amending them as necessary
  - enforcing the escort of persons without independent entry permit
  - application of security service, with patrolling guards

[16] "Prevention of insider threats is a high priority, but leaders and operators should never succumb to the temptation to minimize emergency response and mitigation efforts in order to maintain the illusion that there is nothing to fear" (BUNN–SAGAN 2016: 171).

[17] "In many cases the security rules are so complex that employees violate them inadvertently" (BUNN–SAGAN 2016: 171).

  - applying the DiD[18] principle
  - the redundant and diverse design of the security system, its continued operation in a decentralised, "offline" mode in the event of sabotage
  - restricting access to elements of the security system (e.g. control panel of the walkthrough metal detector, software update)
  - access control with multi-level personal identification, restriction of access and key acquisition rights, adaptation to area and job; strive to ensure that no more licenses are issued than are minimally necessary for the operation of the facility (necessary and sufficient principle)
  - security screening (search of prohibited items) of persons, luggage, vehicle ("remote screening"[19] where applicable) at entry points
  - screening and refusal of entry to suspicious persons and persons under the influence of alcohol or narcotics
  - applying the principles of confidentiality and integrity: restricting physical and logical access to sensitive information (e.g. different levels of software privileges, encrypted communication, use of information splitting (fragmentation of critical information, codes, passwords), digital signatures)
- Vigilance

  Paying attention to changes in employee behaviour.
  - monitoring changes in employee behaviour (e.g. family problems, radicalisation, addiction problems) through daily work contact
  - encouraging the reporting of suspicious persons or incidents to the direct manager and/or the security organisation
  - identification[20] and periodic scanning of critical systems and system components (to detect preparation for sabotage)[21]
  - incentives for cross-checking (holders with permanent entry permit may ask others to prove their identity)
  - periodic reassessment of the trustworthiness, watch the changes of the colleagues (e.g. severe dissatisfaction with his/her private or professional life)
  - training of security staff, e.g. training in the use of security screening equipment (entry, periodic/refresher, non-routine) for operating staff, incorporate possible insider tactics into the training and exercise program
  - periodic vulnerability assessment, assessing the effectiveness of the security system with taking into account the possible insider(s),[22] including with the evaluation of the results

[18] Defence in depth: The increasingly stringent – from the outside towards the installation to be protected – layers of the elements of the security system, which requires more and more time, equipment, knowledge and preparation to penetrate by adversary.

[19] Remote screening: the operator of the screening machine is not in the same room as the luggage, so he/she cannot see who the luggage belongs to (based on the "black box" principle).

[20] "The first step involves identifying those components or areas that could be potentially vulnerable to acts of insider sabotage and are targets within a target set" (Sandia National Laboratories 2019).

[21] For more information on the extreme manifestations of sabotage tools that can be used see Daruka 2012: 33.

[22] Always keep in mind that "any vulnerability assessment which finds no vulnerabilities or only a few is worthless and wrong" (Johnston 2013).

  - updating the protection plan by adapting new vulnerabilities and insider tactics
  - a quality assurance system (periodic and random checks of security system, periodic review of the effectiveness of preventive and protective measures, with testing of equipment at the time of taking over the service)[23]
- Insider inside
  In case if there is still an insider with opportunity for malicious act, protective measures have to face violence: detect, delay and respond, in order to minimise the negative effects of the insider's act and mitigate the caused damage.
  - developing and practicing entry and exit, emergency, security incident management and other plans and protocols
  - installing sabotage-proof, tamper resistant access control, intrusion detection and video surveillance systems at critical locations (e.g. zone barriers, zone barrier hatches, emergency exits) with time-stamped logging and traceability of events and alerts (for incident assessment)
  - maintaining the efficiency of the security system by ensuring adequate availability (e.g. by employing operators and repair and maintenance staff)
  - restricting and slowing down the access to priority premises (access protocol: interlock, time lock, two-person rule[24])
  - application of the "guardian angel policy"[25] for protecting the security staff

Effective defence against an insider becomes more difficult by the fact that most of the time it is only possible to identify the insider if the insider's tactics are known. Insiders' tactics achieve their goal by exploiting a perceived or real vulnerability in the security system. The potential fundamental elements of protection are: the legislation and normative acts; the national security services; the law enforcement structures; the judiciary system; the corporate policy and strategy; regulations (policies, procedures); trainings (security awareness training, entry-level and refresher training); trustworthiness assessment; security system (mechanical protection, integrated intrusion detection, access control and video surveillance system, security service).

Given the creative nature of the human mind and the unpredictability of human actions, possible passive and active insider tactics and protective measures to prevent, identify and mitigate the damage caused by insiders are listed above from the point of view of a security manager of a high security facility.

[23] "Do not assume, always asses and assess (and test) as realistic as possible. Unfortunately, realistic testing of how well insider protections work in practice is very difficult; genuinely realistic tests could compromise safety or puts testers at risk, while tests that security personnel and other staff know are taking place do not genuinely test the performance of the system" (BUNN–SAGAN 2016: 174).

[24] Two-person or "two-man rule is a strategy where two people must be in an area together, thus mitigating insider threats to certain critical areas" (U.S. Department of Defense 2019). The effectiveness of the two-person rule can be increased by rotating teams of two (to prevent over-confidentiality).

[25] Guardian angel policy is an effective defensive measure. The policy means that against a possible insider attack at least one person always has to remain armed and vigilant. It can be applied to form a team of three guards (BUNN–SAGAN 2016: 116).

It is noteworthy, that the most effective measures and actions against insiders can also lead to very radical actions. In these cases, an extreme action usually causes the destruction of environmental factors and has a potential for maximum damage.[26]

By implementing the measures detailed above, the security system will have effective, largely preventive, and better incident detection tools against insiders.

Summary

The fight against insiders is an imbalanced fight. There is no universal or organisation-specific antidote to avoid 100% such attacks while the human factor is present. What can we do? We can strive for prevention, watch our colleagues, implement risk mitigation measures, test, practice and keep the vigilance high all the time. Keep in mind that the threat represented by insiders is a real and major security challenge and never forget that the conspiracies of multiple insiders are also possible.[27]

References

Bunn, Matthew – Sagan, Scott D. eds. (2016): *Insider Threats.* Ithaca: Cornell University Press. Online: https://doi.org/10.7591/9781501705946

Daruka, Norbert (2012): Terroristák és taktikák, avagy védekezz, ha tudsz. *Repüléstudományi Közlemények,* 24(2), 33–41.

Daruka, Norbert (2018): A jövő háborúi az improvizált robbanószerkezetek alkalmazásának tekintetében. *Seregszemle,* 16(2), 7–22.

IAEA (2008): *Preventive and Protective Measures against Insider Threats. NSS-8.* Vienna: International Atomic Energy Agency.

IAEA (2011): *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). NSS-13.* Vienna: International Atomic Energy Agency.

IAEA (2013): *Objective and Essential Elements of a State's Nuclear Security Regime. NSS-20.* Vienna: International Atomic Energy Agency.

IAEA (2018): *Computer Security of Instrumentation and Control Systems at Nuclear Facilities. NSS-33T.* Vienna: International Atomic Energy Agency.

IAEA (2020): *Preventive and Protective Measures Against Insider Threats. NSS-8G.* Vienna: International Atomic Energy Agency.

IAEA (2021): "Preventive and Protective Measures against Insider Threats", e-learning. International Atomic Energy Agency.

Sandia National Laboratories (2007): *Nuclear Power Plant Security Assessment.* Technical Manual, Sandia Report. SAND2007-5591. Albuquerque: Sandia National Laboratory.

[26] Read more about radicalised acts and their means in Daruka 2018: 7–22.

[27] "Conspiracies of multiple insiders, familiar with the weakness of the security system (and in some cases including guards or managers), are among the most difficult threats for the security systems to defeat" (Bunn–Sagan 2016: 156).

Sandia National Laboratories (2019): *Insider Analysis*. 27th International Training Course. New Mexico: Sandia National Laboratory.

Johnston, Roger G. (2013): *Security Maxims: Vulnerability Assessment Team.* Argonne National Laboratory.

U.S. Department of Defense (2019): Unified Facilities Criteria (UFC) Electronic Security Systems. UFC 4-021-02, Change 1.

U.S. Department of the Army (2001): *Physical Security.* FM 3-19.30. Washington, D.C.: U.S. Army Headquarters.