The Third International Regulators Conference on Nuclear Security
From 1 to 4 October 2019
Marrakech, Morocco

Threat Actors: Life Examples of Malicious Attacks

Hadjaro Adam Senoussi

Chadian Agency on Radiation Protection and Nuclear Security

Plan

- Introduction
- Outsider Threats: Types, Characteristics and Trends
- Insider Threats: Types, Characteristics and Trends
- Influential Factors on Malicious Actor Activities

Introduction

- The presentation incorporates some information and facts for understanding the types and the characteristics of the threat actors along with the security measures to reduce the weaknesses and the vulnerabilities in the security system exploited successfully by them;
- The study of the main malicious actors is important to identify their motivation, intention and capabilities as well as their operating methods in order to ensure the people, information and physical assets security through proactive preventive, protective and responsive measures;

Introduction cont'd

- Oxford dictionaries define threat as "statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done;
- Threat actors groups together with the high number of their malicious attacks constitutes important challenges to the national and international peace and security;
- Malicious activities result generally in the damage to people and the industry reputation along with the lack of public confidence on the state' capability to prevent and stop such kinds of activities through an effective regulation;

Introduction cont'd

- Industry leaders and State security authorities cannot claim to have the complete scope of knowledge of threat actors' motivations and tactics and this is because of the clandestine nature of some of them and the secretive style of operation for others;
- Threat actors or malicious actors are divided into two categories: Outsider and insider threats;
- The examples of malicious attacks addressed in the presentation could draw lessons learned for consideration by nuclear community from threat actor's behavior;

Outsider Threat: Types, Characteristics and Trends

- Outsider threat is someone that does not have authorized access to the organization; (IGI Global, What is Outsider Threat, https://www.igi-global.com/dictionary/cloud-security/44679)
- Outsider threat actors involve extremist groups, terrorist groups, organized crime, nation states and target of opportunity;
- They are usually motivated by personal, financial, ideological and political factors to carry out malicious acts such as attempting theft, sabotage or cyber-attacks;

Outsider Threat: Types, Characteristics and Trends cont'd

- Each of outsider threat actors has specific tactics (force or stealth), capabilities and operational methods that permit him to achieve successfully his attack;
- The most dangerous one is an armed group of adversaries with a big number, sufficient capabilities (firearms and explosives) and support from insider;
- It is not exclude that malicious actors look firmly to acquire chemical, biological, and radiological or nuclear weapons;

Outsider Threat: Types, Characteristics and Trends cont'd

- Compared to 2014, the number of terrorist attacks, accompanied with other political violence was decreased to attain 10900 attacks perpetrated by 269 groups or organizations, in which 26400 people killed. Within this number of attacks, 205 occurred in Europe, resulted in 68 deaths and 844 people injured; (START, 2017, Background report, global terrorism in 2107, https://www.start.umd.edu/pubs/START_GTD_Overview2017_July2018.pdf)
- 68% of these attacks are linked to separatists, 16% to jihadists, 12% to left wing, 3% to right wing and 2% none determined; (European Union Terrorist situation and trend report 2018)

Outsider Threat: Types, Characteristics and Trends cont'd

- There are about fifty violent extremist groups around the world, classified as terrorist groups. They employ various kinds of weapons during their attacks to make more deaths and casualties in order to create a terrifying atmosphere. Their operational tactics and strategic goals are not the same. For example, Al Qaeda, Islamic State in Iraq and Syria (ISIS)and Revolutionary Armed Forces of Colombia (FARC); (What are known Violent Extremist Groups? — FBI, https://www.fbi.gov/.../what-are-known-violent-extremist-groups,)

Outsider Threat: Types, Characteristics and Trends cont'd

- ❖Extremist groups are driven by different ideologies in a wrong direction for committing malicious acts marked often by mass murder and destruction to achieve generally political goals;
- ❖The absence of a common definition of terrorism poses an important challenge for the classification of various groups, organizations and state nations actors, which utilize the violence to attain their goals;
- ❖Organized criminal group consisted of three or more persons, motivated by financial or other material benefits and intents to commit malicious acts; (The United Nations Convention against Transnational Organized Crime)

Outsider Threat: Types, Characteristics and Trends cont'd

- Nation-State Actor is an authorized person who works for a third party to commit serious cyber malicious actions aimed at collect sensitive information from other States, business and industry groupings or individuals; (The Unusual Suspects : The Nation State Actor - cyber threats https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor)

- The opportunistic attacker profit from the vulnerabilities found or newly created by him to penetrate in any system and wait for the good opportunity to compromise the security system;

Outsider Threat: Types, Characteristics and Trends cont'd

- In August 2017, a petrochemical plan of a Saudi Arabia company has been targeted by a cyber-attack. The objective of the malicious attacker was not limited only to undermine the plant security system but also to sabotage the plant operations and consequently produce an explosion. According to the cyber security specialists, the high skills together with the enough time and resources used in the attack indicate that the malicious actors were sponsored by a State; (The New York Times, March 15, 2018, Nicole Perlroth, Clifford Krauss, A Cyber-attack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try)
- ✓ *It is clear that political and economic agenda was motivated attackers to perpetrate mass killings through the expected explosion in order to affect negatively the company reputation and public trust in the government*

Insider Threats: Types, Characteristics and Trends

- Insider threat is an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization; (Daniel Costa, Carnegie University, CERT Definition of 'Insider Threat' – Updated, https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html)
- Insiders are divided into; i: Passive who provide information without risk of being detected using deceit or stealth, to support adversaries to launch malicious acts, ii: Active who is ready to furnish information and carry out actions in favor of adversaries using the force or stealth; (IAEA, NSS 8, P. 4)

Insider Threats: Types, Characteristics and Trends cont'd

- ❖ Insider malicious acts include activities related to fraud, theft of confidential or commercially value information, theft of intellectual property or sabotage of computer systems or physical assets;
- ❖ Insider threats include:
- ✓ *Disgruntled Employee driven by the negative emotions like frustration, anger and anxiety;*
- ✓ *Covert Agent who is a trusted employee with an authorized access who secretly provides business information and technology secrets, besides personal and economic information for a third party;*

Insider Threats: Types, Characteristics and Trends cont'd

- ✓*Human Error which is not a malicious act in itself, but unintentionally may lead to facilitate serious malicious attacks;*

- ❖insider threat 2018 report indicate that 51% of malicious attacks come from accidental acts (human error) and 47% of them from (disgruntled employee and cover agent) while 2% of incidents have no determined origins;

Insider Threats: Types, Characteristics and Trends cont'd

- In 1984, for example, two Sikh bodyguards of the Indian Prime Minister Indira Gandhi shot her dead near her office; one of them is a trusted favorite. These bodyguards were motivated by anger against the Prime Minister for her role in combating the Sikh extremist group, especially in the military raid on a Sikh temple in Punjab; (The prime minister of India is assassinated – HISTORY , December 2018 https://www.history.com/.../the-prime-minister-of-India-is-assassinated)
- ✓*The success of this attack could be traced back to nonobservance by the deceased of the security measures, based on threat intelligence and this of course could be connected with the low level of her security awareness;*

Influential Factors on Malicious Actor Activities

- It is not possible to control the intentions and the capabilities of the malicious actors, but it is feasible to minimize the opportunity of attackers and consequently, affects negatively on the quality and efficiency of their capabilities and their determination to perform a successful malicious attack.

- So, minimizing the opportunity could be done through the establishment of an effective physical protection system based on a proactive threat intelligence;

Influential Factors on Malicious Actor Activities cont'd

- The security system refers to "The prevention of and protection against assault, damage, fire, fraud, invasion of privacy, theft, unlawful entry, and other such occurrences caused by deliberate action"; (Business dictionary, security definition, http://www.businessdictionary.com/definition/security.html)
- The effectiveness of the Physical protection regime relies largely on a good regulation and a correct implementation of the physical protection functions (detection, delay and response);
- Intelligence about threat actors' behavior could represent an additional layer to prevent and detect the possible future malicious attacks;

Influential Factors on Malicious Actor Activities cont'd

- The detection system includes: Intrusion sensors; Entry control; Contraband detection; Alarm assessment and alarm control and display;
- Delay system aims to increase the attack timeline while offering the necessary time to the organization to act. Multiple barriers and other physical means such as locks, windows and doors could satisfy this system.
- Response is relating to all actions after the detection to keep the potential impact of a malicious act as low as possible;

Influential Factors on Malicious Actor Activities cont'd

- For insider threat, additional preventive measures should be considered by organizations, using a combination of technical, administrative and physical security measures such as; Trustworthiness of potential employees, escort of visitors, insider awareness trainings and applying the need to know together with the need to access principles to protect information and assets. *unannounced inspections and disciplinary sanctions also, play both preventive and deterrence roles;*

Thank you for your attention