Contribution ID: **200** Type: **Paper**

# Nuclear CyberSecurity considerations.

Cybercrime is widespread and rapidly increasing unabated in many institutions, government departments and in the private sector, as they are at odds in finding effective cybersecurity strategies to combat the new vice. The threats of nuclear attacks backed-up by cyber espionage have become a global issue to which the rate in is rising exponentially.

My concern is to address the challenge on nuclear cybersecurity, backed up by any form of attack. The vulnerability in IoT (Internet of Things) devices, scarce cybersecurity experts, lack of cybersecurity awareness and significant growth in Internet penetration are issues creating new opportunities for different types of attacks. I currently work at Radiation Protection Authority of Zimbabwe, a regulatory body that ensures the safe use of radiation and enforces nuclear security. A lot of sensitive data is captured, stored and consumed and it is our mandate to keep it safe and ensure the CAI (confidentiality, availability, integrity) triad within business processes.

Cybersecurity challenges are relatively new issues in Africa at large, which is unprepared and ill-equipped to handle threats of cybercrime. The risks posed by cyberattacks include exposure of nuclear sensitive information and sabotage of industrial control systems and physical protection systems. The INSSP (Integrated Nuclear Security Support Plan) recognizes the rise of digital intruders and now included the Nuclear Security Area 6 and it is imperative that even though we invest in State-of-the-art physical protection systems, decision makers should also address cybersecurity at their level and cascade it downwards for implementation.

Systems are as strong as their weakest links (human beings if they lack training, but can be great assets if properly trained). Workers at nuclear facilities should develop an optimum cybersecurity culture and only then will we be able to combat digital intruders. The development of the IoT, which enables communication between machines, raises the possibility of appliances being manipulated by hackers remotely. The widespread use of machine-to-machine communication is only likely to boost information misuse and users of these systems should be aware of such vulnerabilities and try and conform to the international best practices of cybersecurity.

Most facilities that handle radioactive materials have inadequate UTMs (unified threat management) systems. Cyber security requirements for a network should include at least Endpoint Protection, UTMs, Radius Server, Logging Software or Encryption. In addition to that, devices should be configured with experts, and training administered to personnel in charge of systems security. Awareness training for all employees is necessary as a foundation and entry point for cybersecurity adoption. Traditional IT security practices like network monitoring and segmentation have become even more critical as businesses and governments deploy IoT devices. Cyber insurance plans should be put in place to cover a variety of costs related to cyber-attacks.

It is very much possible to employ machine intelligence mechanisms to enhance nuclear cybersecurity at facilities. Facilities that use nuclear material have certain information that they have, depending on their sources'categories and their computer interaction patterns, Big Data can be used to make this unstructured data computer readable and enable the effective use of this data by the regulator and the state. Machine learning concepts and Big Data can be used to counter our problems within SOCs (security operations centres) as well as enhance nuclear security detection architectures. Machine learning algorithms can be used to support Big Data by learning the vulnerabilities and ransomware trends, and coming up with ways to guard against digital intruders. There are over 1000 facilities in Zimbabwe that use radioactive material, and a security breach of any of these facilities could cause a catastrophic nuclear security accident. The risk of such an event is always there and the challenge is that, RPAZ has no idea as to which facility is engaging in practices that can compromise nuclear security. Big Data is the can then be used to analyze digital trends within organizations and use machine learning algorithms to come up with ways to determine facilities that are bound to compromise nuclear security and proactive measures are taken immediately as opposed to reactive measures, thus, ensuring nuclear security in Zimbabwe and the world at large.

Nuclear Cybersecurity is one of the most urgent issues worldwide. Computer networks have always been the target of criminals, and the danger of nuclear security breaches will only increase in the future as these networks expand, but there are sensible precautions that organizations and states can take to minimize losses from those who seek to do harm. With the right level of preparation and specialist assistance, it is possible to control damages, and recover from a cyber breach and its consequences. Cyber Security awareness is important in order for companies and individuals to keep on guard against attacks. It may not happen imminently, but eventually a breach is bound to suffice and one has to deal with the fallout.

## State

Zimbabwe

## Gender

Male

**Author:** Mr NDALAMA, Leenold Tinashe (Radiation Protection Authority of Zimbabwe)

**Presenter:** Mr NDALAMA, Leenold Tinashe (Radiation Protection Authority of Zimbabwe)

**Track Classification:** CC: Information and computer security considerations for nuclear security