NUCLEAR CYBERSECURITY CONSIDERATIONS

Leenold Tinashe Ndalama
CEH | CISCO | SOPHOS | MSc. (Stellenbosch University)
Zimbabwe
nleenold@yahoo.com nleenold@aol.com

Abstract

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.

1. INTRODUCTION.

Radiation Protection Authority of Zimbabwe is a regulatory body in Zimbabwe that ensures the safe use of radiation and enforces nuclear security within the country. A lot of sensitive data is captured, stored and consumed and it is its mandate to keep it safe and ensure the CIA (confidentiality, availability, integrity) triad within business processes. CyberSecurity has become a global issue and it is imperative that we include it (Nuclear-CyberSecurity) in our strategic plans on how to combat digital adversaries and safeguard nuclear-sensitive information.

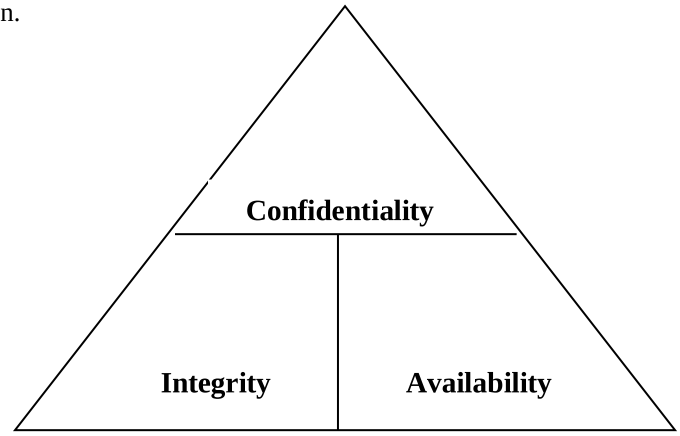

FIG 1: The CIA Triad

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, sabotage of industrial control systems and physical protection systems. The INSSP (Integrated Nuclear Security Support Plan) recognizes the rise of digital adversaries and now included the Nuclear Security Area 6 (NSA 6). 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 (untrained human beings, 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. CyberSecurity 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 source 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 500 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 can then be used to analyse 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. CyberSecurity 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.

2. IMPLEMENTATION.

These are CyberSecurity implementation recommendations to achieve minimum security architectures commensurate to the kind of Nuclear-Sensitive Information (NSI) that a facility holds.

NSI is classified based on the source categories, that is, category 1-5 and it spans from low to high risk, with category 1 being the category with the highest risk. Each facility that handles NSI of any category should at least have CyberSecurity controls that preserve the CIA triad at all times. The minimum requirements should be as follows:

- Policy – every facility should put in place an information and computer security policy that adheres to the standards and best practices. This policy should be enforced. IAEA Nuclear Security Series publications should be referenced when developing policies and Integrated Management Systems so that all business processes conform to the required standards and specifications. It is also important that facilities have DRPs (disaster recovery plans) in place so that in the case of an incident, there is a welldefined plan that communicates and clarifies all the roles and responsibilities for smooth sailing.

- LAN (local area network) – each facility should have a well-defined LAN so that all weak points can be identified and dealt with, thus reducing the attack surface. Remote branches that handle NSI should have access to the information via VPN (virtual private network) so that the connection is secured since it passes through the public domain. Segmentation should be well implemented to avoid malware propagation in the case of an emergency.

- UTM – considering the size of the organization and the amount of packets that traverse the network, a facility should have firewalls and security tools that cover the infrastructure. A UTM should be configured as per the policy and monitored to keep track of all the breaches. Considering the size of the organization, it is recommended to have a SIEM (security information and event management) tool that monitors network activities and correlates event notifications with CyberSecurity concerns so that incidents are attended to as they happen.

- Endpoint security – the use of an anti-virus alone has proved to be ineffective since it is susceptible to zero-day-attacks, so it is imperative to have Endpoint Security tools that communicate with the firewalls, sandbox and threat intelligence platforms. This will reduce unknown attacks by quarantining suspicious files into the sandbox (an emulation of a real endpoint) so that the activity is monitored and if it is a virus, the definitions are then synchronized with the threat intelligence server and protect everyone under it.

- Licensed software – statistics show that most of the software used in Africa are unlicensed and this poses great risks to information and computer security. Software licensing should be taken seriously and prioritized to curb risks that come along with their use. If possible, the government should intervene and consider volume licenses for facilities that use the same tools. It is my recommendation (funds permitting) to abscond from using free tools or software in a move to avoid premium software since free software is prone to attacks and has limited product support.

- Awareness – a significant number of computer users at facilities in Zimbabwe are not aware of CyberSecurity and the associated risks. Investing in state-of-the-art security systems will not combat anything if the users are not impacted with a CyberSecurity culture, so it is imperative to conduct awareness programs for all users so that the security culture is boosted. Employees at facilities as well as the regulatory bodies should be CyberSecurity conscious and that is attained through awareness programs and refresher drills that constantly remind them how to behave on the cyber-space. It is also important for the regulatory body to include CyberSecurity in the RSO (radiation safety officer) training curriculum so that all the RSO understand and appreciate the role and implications of CyberSecurity. These awareness programs will then translate to a sound security culture that has a lot of ad vantages, some of which listed as follows:

    1. The level of security increases as the CyberSecurity culture is built.
    2. If CyberSecurity levels increase, this also increases the level of nuclear safety to some extent and this is the ultimate goal.
    3. This then leads to a reduced number of CyberSecurity breaches, thus, reducing disaster recovery costs to the organisation.
    4. Positive outcomes will increase employee satisfaction and also increase their performance levels since they take pride in it.

    Setting up a strong and very much coordinated information and computer security culture as a segment of the general security culture is a fundamental part in any powerful security plan.

- Management commitment – Ultimately CyberSecurity is the responsibility of top management and they should understand and prioritize the implementation of the requisite controls to house certain NSI. Everyone plays an important role in implementing and upholding CyberSecurity, so it is of paramount importance that everyone understands their role and the required competencies to execute the roles.

- NSI classification model – There should be a model that identifies all the NSI at a facility and the clearance levels for everyone. All security controls should be implemented based on the model. The regulatory body of a particular country should have regulatory guidelines for developing the model that will be adopted by all facilities so that they can customize to suit their industry and organizational size.

- Security controls. Sound security controls are those that are not lax, preserves the CIA triad and ultimately attain the set objectives. Implementing the CIA triad entails that information is kept confidential, with no unauthorised modifications and is always available as and when required. The least privilege principle and separation of duties should be implemented within these controls so as to ensure information and computer security.

- Logging software. An audit trail of any interaction with any system plays a pivotal role when handling a breach. System logs and even physical access logs should be maintained in order to protect individuals, information and the organisation at large.

- Regular backups. Fault tolerance is possible when there are reliable backups for the systems. It is important to do regular backups and to carryout drills for backup restoration to check for any errors and inconsistencies that may occur.

- Pre-licensing inspections for various authorizations should include meeting the requisite CyberSecurity requirements for a particular category before authorization. This stance will enforce CyberSecurity compliance for all facilities.

- Nuclear Security Detection Architecture (NSDA). This is the responsibility of the state and it is imperative to address the CyberSecurity issues at that level, so that commitment and direction cascades from the top to the bottom of the chain. IAEA introduced the NSA 6, showing its commitment and understanding of the underlying CyberSecurity considerations within nuclear security. Traditional security models need to be revamped to enable Cyber-Resilience within business processes and standards of operations in any setting.

- Facilities need people who are well trained to work as security analysts so that all the critical security decisions are made and implemented so as to maintain information and computer security at all times. It is known that there is a shortage of CyberSecurity personnel, so facilities should make notable efforts to equip their staff with proper knowledge and skills to handle NSI. IAEA already has training programs that aim to capacitate facilities with the requisite skills and it becomes easier for facilities that have little to no resources.

- Computer security assessments. The relevant regulatory body should carryout computer security assessments to ensure that facilities are compliant with the CyberSecurity regulations commensurate to the NSI that the facility has. This stance will significantly enhance compliance and a clear picture of the attack surface of the whole country.

- Risk profiling - these assessments can also be viewed as ‘vulnerability assessment’ where external experts come and assess the systems and business processes for weaknesses that can be manipulated. It is very much important to know the vulnerabilities in your systems and business processes so as to have a real picture of the risk register and take necessary measures to prepare for the risks. Risk should be kept at acceptable levels that will not compromise sensitive information or continuity of the business, so anything that compromises business continuity and sensitive information should be dealt with.

These implementation recommendations will go a long way in enhancing information and computer security at facilities that handle nuclear and/or radioactive material. The main goal is about building a CyberSecurity culture and only then will implementing a sound architecture be successful. The risk of a CyberSecurity breach is always present and controls are put in place to reduce the probability of an event happening, by minimizing opportunities for compromise.

3. RECOMMENDATIONS & RESEARCH.

These recommendations and research pointers are at a broader spectrum that can enhance CyberSecurity at large and perhaps be employed within the Neclear-CyberSecurity fraternity.

There is a new concept known as the *zero-trust security model*, implemented with micro-segmentation. This is when systems are configured not to trust anything, this entails that authentication is always done and this reduces breaches in some way. Micro-segmentation then helps to prevent malware traversal across the whole network. This is an effective model to implement at facilities with very sensitive nuclear information (category 1&2) since the interception of such information would be drastic. This however requires a great deal of investment in topspec equipment that will ensure efficiency and effectiveness since the zero-trust security model has a lot of overheads.

I think the use of Machine Learning (ML) in Nuclear-CyberSecurity is the next best thing concerning combating threats that are very much sophisticated. Using unsupervised learning algorithms, it is possible overtime to learn patens of a nuclear-sensitive information breach and alarms can notify potential breaches before they occur. It is also possible to automate certain incident responses using supervised learning and reinforcement learning so that if a particular event occurs, the system has learnt how to respond and will respond. However automation has a challenge that in some cases you need reasons for certain actions of which this is difficult to obtain from AI (artificial intelligence), so it is imperative to limit automation to simpler tasks that are not critical, also implementing a graded approach.

Upon realizing that nuclear security can be enhanced by regional and global collaboration, the use of the ITDB (incident trafficking database) should extend to sharing of knowledge concerning nuclear cyber-breaches so as to prevent the use same techniques in different places. A central threat intelligence platform that serves as a repository of information concerning failed and successful breaches will go a long way in equipping facilities with the relevant tools to combat new vices. It is also important to conduct national meetings to discuss issues related to Nuclear-CyberSecurity on regular basis so as to enhance awareness, knowledge transfer among locals and to be abreast with the latest advancements in CyberSecurity.

Information and computer security at facilities that handle nuclear and/or radioactive material is very much possible and it requires a great deal of commitment to be a success story. The IAEA in collaboration with experts in nuclear security and CyberSecurity can work together to develop customized tools that particularly address CyberSecurity issues that are unique to NSI and related facilities. Collaboration among facilities, regulatory bodies and countries should be implemented and supported so that knowledge can be shared and transferred, combating these digital adversaries. Understanding that computers have since been introduced within our processes, we have to appreciate the risks associated with using them even though the benefits outweigh the costs. Awareness programs are at the centre for success and it remains the responsibility of everyone to play their part towards the success of Nuclear-CyberSecurity.

There is a trend of CyberThreats that has been observed over the years and it is important that I also give a few highlights here that will probably happen as follows:

- Sophisticated tools are being developed every day and with the introduction of Artificial Intelligence (AI), adversaries will come up with complicated ways to breach systems and this will be difficult to detect and respond to.
- Spear phishing. This is when phishing attacks are target for particular individuals. Generic phishing does not really yield or meet the set goals, hence adversaries will increase the number of spear phishing so as to gain the information they want.
- Considering the types of ransomware that are now available, and the rate at which technology is moving, more ransomware will be introduced as time progress.
- Now that most facilities have little to no care concerning CyberSecurity, more digital adversaries will tag along and this means more breaches.

Concerning these trends and prospective actions, organisations should take a proactive stance to protect themselves against current threats and those that are likely to come. This entails that it is important to invest in research and development and also to keep abreast with the technological advancements within the CyberSecurity fraternity.

4. BIBLIOGRAPHY.

Arnold, Rob. Cybersecurity: a Business Solution: an Executive Perspective on Managing Cyber Risk. Threat Sketch, LLC, 2017.

Bejtlich, Richard. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, 2013.

Computer Security at Nuclear Facilities: Reference Manual. International Atomic Energy Agency, 2011.

Conducting Computer Security Assessments at Nuclear Facilities. International Atomic Energy Agency, 2016.

Géron Aurélien. Hands-on Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems. O'Reilly Media, Inc., 2019.

Gibson, Darril. CompTIA Security+: Get Certified Get Ahead: SY0-501 Study Guide. YCDA, LLC, 2017.

Gilman, Evan, and Doug Barth. Zero Trust Networks: Building Secure Systems in Untrusted Networks. O'Reilly Media, 2017.

Zinatullin, Leron. The Psychology of Information Security: Resolving Conflicts between Security Compliance and Human Behaviour. It Governance Pub, 2016.