ALTERNATE MINING SECURITY MANAGEMENT

Engr. Amosu Cyril Olumuyiwa

Department of Mineral and Petroleum Engineering

Yaba College of Technology, Yaba.

ABSTRACT

As mine operators begin to integrate enterprise-wide systems in order to gain efficiencies, security risks are increasing. To combat this, mines must implement real-time visibility and security solutions designed to reduce risk and build operational resiliency. To withstand market volatility, mine operators must maximize efficiency while incorporating security best practices. The vast areas covered by mining operations present several security challenges that are not necessarily faced by most other environments - chief among them the ability to provide effective perimeter protection and surveillance. This paper looks into security, the issues that confront it and possible best solutions.

KEYWORDS : Security, Management, Monitoring, , Devices, Danger, Risk, People, System, Implementation, Solution

---

INTRODUCTION

SECURITY:

Merriam-Webster defined security as the quality or state of being free from danger, risk or threat. According to vocabulary dictionary, security means safety, as well as the measures taken to be safe or protected; and Collins dictionary defined it as all the measures that are taken to protect a place, or to ensure that only people with permission enter or leave it. It covers three (3) major areas (see figure 1.) which are:

(i) **Physical Security:** is the protection of people, property and physical assets from actions and events that could cause damage or loss.

(ii) **Information security:** is a set of practices designed to keep personal data secure from unauthorized access and alteration during storing or transmitting from one place to another (Robert, 2020)

(iii) **People and processes:-**

(a) **Personal Security:** is a general condition that occurs after adequate efforts are taken to deter, delay, and provide warning before possible crime, to summon assistance, and prepare for the possibility of crime in a constructive manner (US Legal, 1997).

(b) **Cyber Security:** is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks (Kaspersky, 2021). It has about seven (7) Information Security controls, as shown in figure 2 and Table 1.

SECURITY MANAGEMENT:

Security Management is the identification of an organization's assets (including people, buildings, machines, systems and information assets) followed by the development, documentation, and implementation of policies and procedures for protecting assets (ASIS, 1997). It is a form of trusted distribution of access control that allows one principal to delegate some access decisions to other principals (Ninghui et al, 2005). It varies according to the expressive power of the management language of that there is no legislation that regulates the information security liabilities of the public organizations (Sevgi and Bilge, 2010)

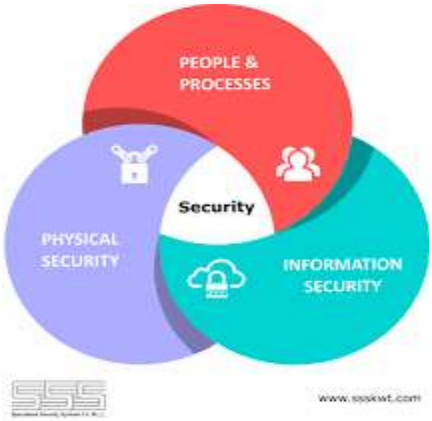


Figure 1: Security Areas (ssskwt.com)

Figure2: Information SecurityControl (diacritic.com)

TABLE 1: Sample security practice components (Dams Sector Security Guidelines, 2015)

Physical	**Information**	**People and Process**	
		Personal	**Cyber**
Assessment	Sensitive Information Classification	Background Screening	Network Access Control
Security Plan	Protocols and Procedures	Training	
Protective Measures	Information Sharing Mechanisms	Exercise and drills	Abnormal Condition Detection
Response Forces	Suspicious Activity Reporting	Response and Recovery Planning	Disruption Response
Defence In-Depth			Asset Recovery

SECURITY MANAGEMENT:

It has 6 (six) items for its functionality which are unavoidable (see figure 3) which are: (i) discover; (ii) Prioritize; (iii) Assess; (iv) Report; (v) Remediate; (vi) Verify.

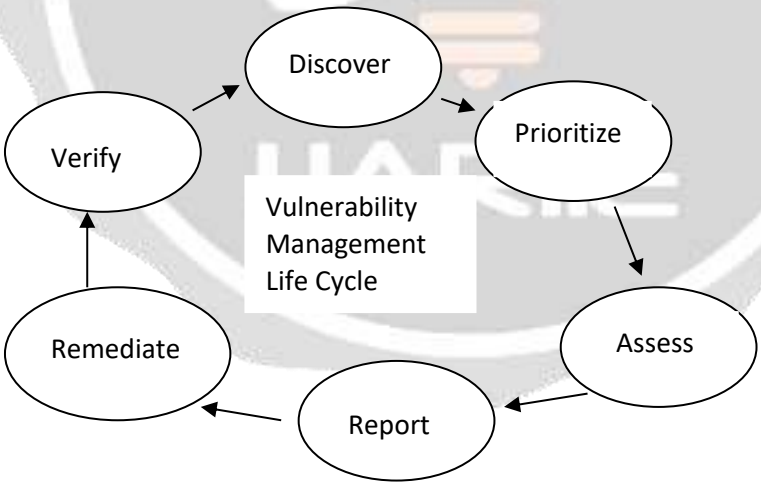


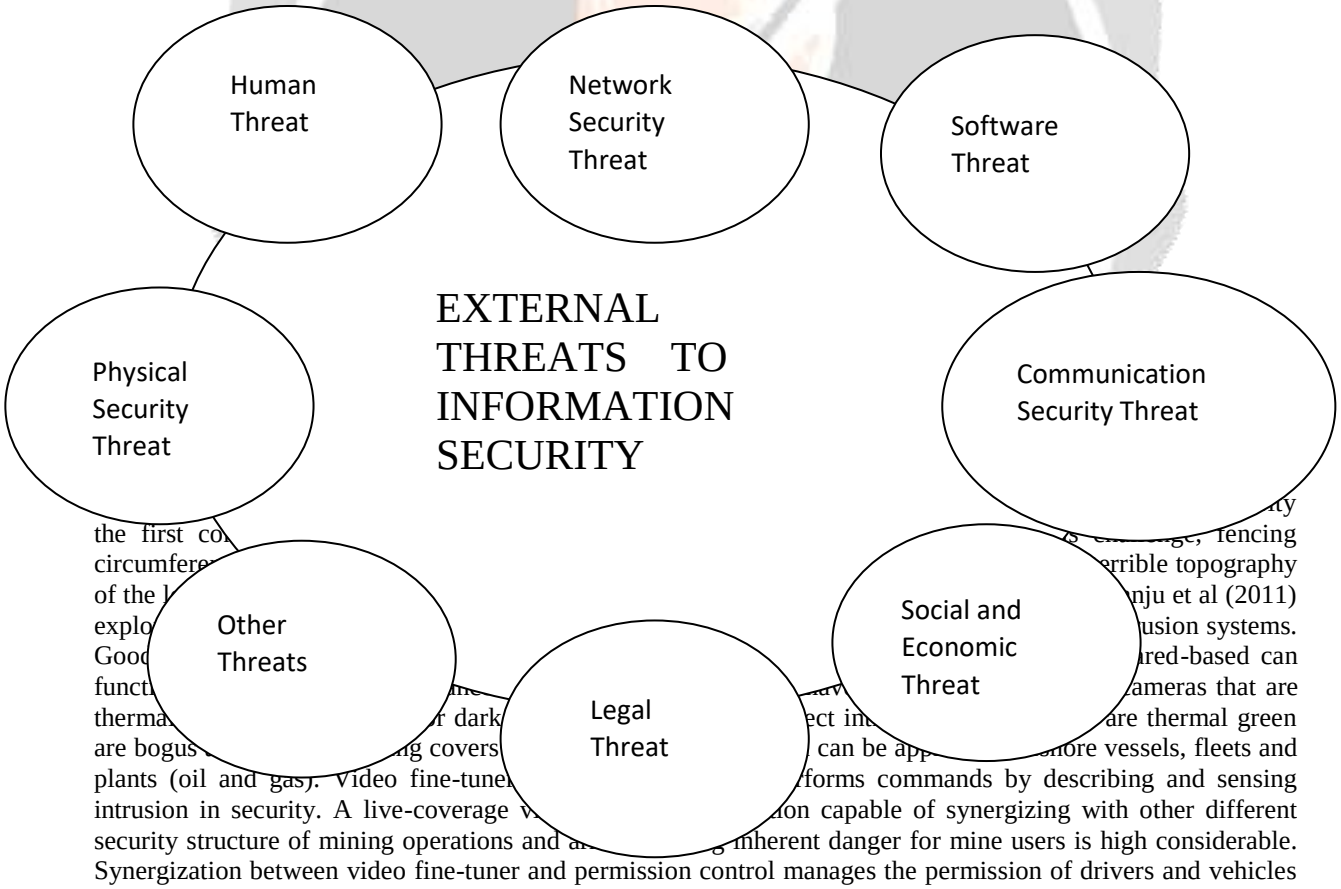
Figure 3: Vulnerability Management Life Cycle (securityvern.com)

Mining supports the foundations of a nation, as economies can rely on the vital resources on earthed. Ahmad et al (2014) report that organizations are in a preventive mindset when it comes to information security measures. In the presence of big data mining, the information security and privacy preserving of the sensitive information play an important role (OndrejVyborn, 2006). While the mining industry contributes greatly to worldwide economy, it faces threats requiring comprehensive security and safety solutions. Aleem et al. (2013) present approaches to mitigating blended threats in the areas of physical security and information security. Patel et al. (2010) presented a survey on the comprehensive state of intrusion detection and protection systems. These systems should use a combination of techniques to assist them in determining the actual intrusion from normal activity. Puzis et al (2009) studied effectiveness of attacking anonymity through collaborating eavesdroppers.

Since the world's mining output will grow 3.9 percent each year to 38.9 billion metric tons by 2011. China's output alone for aluminium products has tripled in the past five years, reaching 12.4 million tons. The fastest growth is expected in developing regions, notably China, Southeast Asia, Latin America and Africa. Australia, the third largest producer of gold globally, will grow due to strong demand from China and India. Worldwide demand for precious metals and copper benefits the African mining industry. South Africa's economy thrives on mining and it is the biggest producer of platinum and one of the largest suppliers of gold in the world. It also produces coal and diamonds. High-value minerals require security and worker safety, since mines are harsh environments. South Africa pride in some of the deepest mines in the world. Some gold mines reach deeper than 3,000 meters, with speculation of digging below 5,000 meters, which means that safety is a huge and expensive issue (Going Deeper, 2016).

THREATS AND SOLUTIONS

Some of the biggest security issues for mines are perimeter intrusion, illegal mining and theft. Securing equipment and ensuring employee safety are also important concerns. Dust, humidity, fog, low light, extreme temperature and weather conditions are issues at mines. There are about eight (8) types of external information security threats (see figure 4). Ahirwar et al (2011) discussed that human-related incidents are the cause of a large number of security threats, and that the constantly evolving developments in technology make it difficult to keep up with new threats. Compared to commercial-use security systems, mining security systems must work in harsh environments. Cabling technique is different for different mines, since drilling or attaching cables to rock can only be done by engineering personnel. Pre-installed infrastructure cabling provides power and communications for conveyor systems or vehicle workshops to most underground points since high level security is required, solutions must be tailored to each mine. Open-pit mines based on authority and risk levels put emphasis on access control, while underground mines with a higher requirement for safety puts emphasis on people location management. For volatile environments such as gas and oil refineries, international security-rated equipment would be required. Offshore mines focus on meeting and maintaining safety standards (Going Deeper, 2016).



the first co… …ity
circumfere… …errible topography
of the l… …njju et al (2011)
explo… …usion systems.
Good… …ared-based can
funct… …ameras that are
therma… …r dark… …ect in… …are thermal green
are bogus … …ng covers… … can be app… …shore vessels, fleets and
plants (oil and gas). Video fine-tune… …forms commands by describing and sensing
intrusion in security. A live-coverage v… …on capable of synergizing with other different
security structure of mining operations and a… …inherent danger for mine users is high considerable.
Synergization between video fine-tuner and permission control manages the permission of drivers and vehicles
(Going Deeper, 2016).

ILLEGAL MINING

In Africa, the toughest challenge for mining includes pilfer miners and unlawful mining events. Pilfer miners illegally reside underground of mines and schemes across mine sites unannounced, hereby, disrupting the mine framework. They usually risk mercury poisoning by making use of the deleterious mercury for gold extraction, Unlawful mining quantity can be tremendously reduced using the security systems, even though it cannot be

totally avoided, but well-monitored supervision through synergized security can reduce the danger of unlawful mining options (Going Deeper, 2016).

MINERAL THEFT

In South Africa, about a handful of the gold that is exploited is carted away before it can produce gain for the mining firms. To forestall this crime, most focus points at control of access and detection of disruption for facilities and machineries used for storing, processing made available. Theft can be minimized with due access control, biometrics, and detectors of metal, attendance checks, boom gates, Radio Frequency Identification (RFID) access control, background and period control. Commencing daily activities, miner workers begin by going through a mining elevator; replace their work gear and dresses in the mining underground tunnels. These equipments of video surveillance, monitoring access control, turnstile alternatives and biometrics are assembled around the mine. Only qualified individuals are allowed on site for labour intensive areas is ensured by biometrics capture, as card-based options without it could be perceived as scam. Fingerprint, retinal and palm vein scanning are popular recognition methods used at mines. Turnstile alternatives are often built together with attendance - and- time management, biometric and video surveillance. No unauthorized person can go beyond the entry spot, since turnstiles only allow persons, one at a time. Portable trace detection scans ensure no resources are taken away illegally especially for the security of everyone entering or leaving the mine location. These helps to track mine workers and its assets in order to ensure safety and security. It is of note that swipe cards or passive tags operated at the surface mine are not suitable in underground environments because they impede mobility through the mine and add to productivity loss. A built-up system for tracking which uses the data from tagging systems (both passive and active) is expected to inter-connect the surface, sub-surface and underground systems (see figure 5).

Figure 5: Monitoring for underground mine tracker (real-trac.com)

While guarded surveillance and video capture can be utilized at the surface and underground, synergized options can monitor attack on the surface by applying biometrics of eye or fingerprint, and also intelligent detection of circumference of the surrounding. All of these activities can advance with built-up security options (Going Deeper, 2016).

EQUIPMENT SECURITY

Result-oriented mining security aids mine operators to delve and look into critical issues bordering around the operation's improvement. Operators can guard various instruments and their points of the utilization process with detection devices such as cameras strategically positioned throughout the mine. Monitoring and securing equipment like mine vehicles is relevant and beneficial because some of them runs into millions of dollars and are expensive. Tracking and Tagging of Asset(s) is a vital example for mines and as such must be rugged and reliable. The two must be certified in methane-bearing coal mine-sites when used. Sensor options (collision alert technology system) like onboard vehicle collision can also be used to protect property. They pick –up quick signals of hazards in the path of the vehicle and warn drivers for imminent collisions hereby preventing dent to the vehicle and safe-guarding mineworker. (Going Deeper, 2016).

EMPLOYEE SAFETY

The primary security objectives and aim is safety and productivity of mine workers. This is an issue for tough mines locations, especially for mines that exploit mineral products like gold, coal, tin, potash, and so on. Access control, surveillance, sensors and RFID with management software and regulations ensure worker safety. The first step is to verify that only authorized personnel who passed safety inductions, medical checks, training and has renewed license is granted access control at mines. The second step which is essential for protecting employees is to monitor the work zone using underground video monitors which aids to track the safety of a miner by: monitoring rock falls or its accidents in real time capture; increase search speed and rescue period;

pick up signals of hazardous substances, explosives or gases (i.e. when a worker is in a hazardous area or is close to it; and help to suppress the operations of illegal miners. For location points or spots that video coverage or capture cannot reach, wireless gas sensor signal detectors (see figure 6) are an alternative to monitor the release of methane gas and other hazardous substances.

Figure 6: Wireless Multimedia Sensor Network (indiamart.com)

In case of an accident, the operational safety and health (OS & H) solution must detect miner workers by the security measures mentioned earlier (see figure 7).

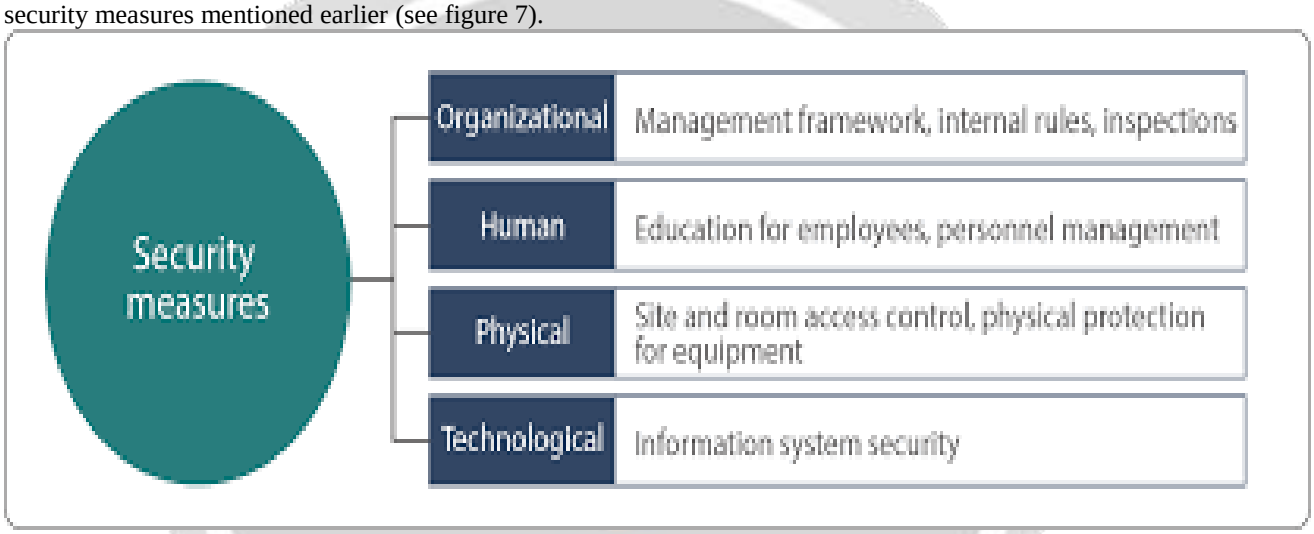


Figure 7: Security Measures

The antidote should produce quickly back-up records by making available information of the precise count of personnel in the control room at any given time. For instance, In South African mines, biometrics is used to report the number of people coming in and going out of a particular mine shaft and area in order for operators to know when it is safe to blast in particular space. (Going Deeper, 2016).

EMPLOYEE HEALTH

Apart from issues bordering on safety and security of mining operations, the health conditions of an employee may deter the productivity of work and raise the occurrence of accidents. Catering for the health and welfare of staff can provide a safe and efficient mining operation. Fatigue management of workers and testing their blood should be synergize with the controlling of high exposure to hazardous materials in mines. By a set date, the workers could also be strictly instructed to visit the medical facility for blood testing and other check-up. Employee payrolls, health, safety and legal compliance can be maintained by biometrics. It can also be installed to record the level of nutrition gotten by each worker at eating halls, ensuring them a healthy diet to be fit for work (Going Deeper, 2016).

THE COST OF UNSCHEDULED DOWNTIME

Many production processes rely on automation in which a malfunction in just a single device can have a great negative rippling effect across the entire system, as a result of equipment breakdown and failure. Equipment wear-and-tear and unplanned downtime are critical and can sidetrack even successful operations. The total cost of unscheduled downtime in mining is estimated at 15 times that of scheduled activities. This unplanned downtime happens for different reasons which range from friction in non-captured signal detection to technical cyber-attacks. This makes tracking the state of the entire instruments in a mine to be difficult in real-time. Basically, mining operators conduct assessments of production system operations monthly.

CYBER THREATS TARGET CORPORATE DATA

Attempts to gaining access into corporate data base of mining companies are the targets of some other corporate interest groups and countries. Such effrontery can be perceived in the prospecting of research and development,

and other business ventures circumstances to gain undeserved benefits. This has prompted for stiffer scrutiny in mining companies, especially to curtail their impact on mining operations and its working territories. Traditional techniques and approaches are not enough to protect data but that improving security should start with the education of database specialist was discussed by (Blake, 2015). Processing huge amount of data with latest cutting edge technologies can help companies to save money and time besides improving their financial status (Chris, 2012). Its appropriate exploitation will help in mining as much as possible for prioritization (SAS, 2012). In Australian for instance, the mining radio communication and technology manufacturer, CODAN revealed that it took a big hit from cyber hackers operating in China that stole the design of its metal detector and flooded the market with cheap and fake versions. This forced CODAN to slash the price of the detector by 50 % in order to compete and this resulted to losing about 80% of its profit in that year. Also, NORSK HYDRO which is one of the widest manufacturers of aluminium globally, got a crippling cyber-attack blow, and lost about $70 million in March 2019 which forced it to switch some of its mining operations to manual, and also to abandon its plants, after its computer networking capacity was paralysed. (Going Deeper, 2016). Cyber-security, which involves protecting both data and people, is facing multiple threats, notably cybercrime and online industrial espionage, both of which are growing rapidly (Kouroush and Saeidm 2016).

GOVERNMENT-REGULATIONS

Security and safety are integral parts of any business. So, the mining company management are continuously aware of the expenditures tied to loss of lives (i.e. worker), loss of material, equipment and the failure of the safety structure or system put in place. Improving the level of security and safety buttresses government regulations, saves money, enhances productivity, decreases infrastructural losses and reduces downtime in production. Government regulations averts heavy fines and prison sentences for users and avoid substantial expenses related with accidents in mining which exceeds that of other industries (Bajpayee, 2004). For instance, Security Sensitive Ammonium Nitrate (SSAN) makes the rules available for explosive storage facilities that should be complied with. Other worldwide organizations that set rules and policies for public safety in mines and employee OHS (Operational Health and Safety), EHS (Environment Health and Safety), HSE (Health Safety and Environment) and OHSE (Operational Health Safety and Environment) (Going Deeper, 2016). Insufficient capacity to monitor and implement regulations may lead to the potential by- passing of governments as key regulatory agents and consequently further undermining their legitimacy (Bonnie, 2006). In situations of conflict, in order to ensure security, mining companies may turn to private security companies or co-opt armed groups to protect installations, thus contributing to further insecurity.

SECURITY CHALLENGE

Three challenges confronted by mining security include:

(i) **Huge costs of the installation of best available technology:**

Though expensive, security in mining must be improved upon with high effective subsurface control at the points of entry and exit of mine tunnels. Mine surveillance is not considered as a tenable alternative for some underground mines because of lengthiness of tunnels and harsh situation and also because such tunnels extends to hundreds of kilometres and cannot be monitored by cameras effectively. Video and Alarms can be installed along the boundaries of mine-sites to provide useful integrated solution to operational attacks of any sort (Mining, 2019). The entire cables used for mining purposes need to be kept in air-sealed or waterproof substances to prevent dust and other particles from destroying them. It should be ensured that explosion-proof devices are erected with the right cable management systems.

(ii) **Tough weather:**

Temperatures could exceed 45 degrees Celsius at the depths of some mines, and some mine environments are continuously humid, damp and moist, which limits the technology that can be used. Mine operators require tight waterproof units, vibration dampers, which can withstand differing range of temperatures.

(iii) **Availability of large space:**

The large area in the mine-site poses a problem to security. It makes it difficult to secure cost effectively with barriers. Illegal miners still find ways to navigate the mines through mining and residing underground, even with the most holistic security options put in place.

ADDRESSING AND OVERCOMING CHALLENGES IN MINING SECURITY

The steps involved in the managing of site-security matters include:

(i) Identifying and evaluating all the factors of risk that is applicable to every site.

(ii) Constructing peculiar security - plan for mine-site as a document of operational resource to display the aims, tactics and duties needed to meet the safety of the site, health of workers and security goals. Any successful plan of security for a mining environment must factor in a total security training program for the mine-site.

(iii) Providing of an experienced security team and creating technology, processes and systems to support in the maintenance tradition of safety, in order to cut-down undue debt to stealing and unpermitted entry to the mine.

(iv) The right risk management tools, enlightenment and training needed for identifying hazards; and also taking the right actions must be given to workers when such hazards are discovered See figure 8.

Figure 8: Risk management tools (perez-moris.com)

(v) Making available result-oriented communications and customer service procedures which include processes of problem resolution and tactics to prevent upsurge (Gupta and Hammond, 2005).

(vi) Enlightenment in the use of security emergency management, its procedures and equipment, bag and vehicle searches, auditing, visual and patrols education, incident response, investigation, report writing, certification and communication of all security-associated matters must be given to staff.

REDUCING THE COST OF SECURITY OPERATIONS

Implementing and maintaining security is a very expensive system. Nonetheless this expense could be paid on instalment by synergizing process, procedures, network, and instrumentation constructed for security into zones of the mining operation. Also on the increase is the application of technology formed for specialized work used to assist with varying large arrangement of duties within a mine-site by some companies. Examples of such technologies include high-speed broadband, digital radio and closed-circuit television (CCTV) (John B, 2012).

FUTURE TRENDS

Since the economic recession and depression has affected the growth of the mining industry, cost-effective security is in relative demand. Synergized solutions and automated mining processes helps to cut-down the amount of labour needed while maintaining the same strength of security. With new services and systems made available recently, the

usability and availability problems are addressed (Moens, 2012). Improved integration invariably signifies greater efficiency in operation which hereby increased savings of customers on the long run. Common-place and trend are Security software synergized with Enterprise Resource Planning (ERP) software. Systems of access control connected to software of human resource share the data of staff, such as alcohol drinks, drugs and blood testing need. This instrumentation could replace hand labour which uses machinery in places of high-risk. Mine operations should plan to adopt alternatives such as code-control gates and turnstiles or PTZ cameras for remote visual verification through a single control room (Mining, 2019).

CONCLUSION

Security which is the quality or state of being free from danger, risk or threat is important to note in mining, to proffer best safety practices and measures to protect a place, or to ensure that only people with permission enter or leave it. While the mining industry contributes greatly to worldwide economy, it faces threats requiring comprehensive security and safety solutions. There are lots of influx and inflow of people and information, physically and on the internet. This capacity is been threatened globally, by illegal means and theft methods. To encourage safety, and prevent downtime, surveillance, monitoring and integrative security solutions should be adopted. These threats come as human, network security, software, physical security communication security, legal security, socioeconomic security. Several devices (like Installed CCTV, Digital Radio of high resolution, High Speed Broad Band, Video Monitoring Surveillance Security , Biometric Data Security , Barriers Turnstile Access, Boom Gates, RFID Access Control , X-ray and Metal Detector , PTZ Camera are recommendations to be employed to check security, in the mine-site. Adequate security plan; right risk management tools; appropriate enlightenment and training program for workers; strategic technology, processes and systems for a mining environment must be factored in to cut-down undue debt to stealing and unpermitted entry to the mine.

REFERENCE:

1. Mining (2019): Securing Operational Resiliency through ICS Visibility and Cyber Security, Nazomi Network Industry Brief.
2. Going Deeper (2016): Security at Mines A & S International.
3. John B.,(2012): Overcoming Security Challenges in the Mining Sector.
4. Kouroush J. and Saeid M. (2016): Business Management Dynamics , Cyber Security Management – A Review, Vol.5, No.11, pp.16-39.
5. Ahirwar D., Ahirwar M. K., Shukla P. K., and Richharia P., (2011): An analytical survey on network security enhancement services. International Journal of Computer Science and Information Security, 9(3), 259-262.
6. Blake E. A., (2015): Regulatory compliance, network, and database security – A unified process and goal, Journal of Digital Forensics, Security and Law, 2(4), 77-106.
7. Ahmad A., Maynard S. B., and Park S., (2014): Information security strategies - towards an organizational multi-strategy perspective, Journal of Intellectual Manufacturing, 25, 357–370.
8. Aleem,A., Wakefield A., and Button M., (2013).: Addressing the weakest link - Implementing converged security. Security Journal, Vol., 26(3), 236–248.
9. Gupta A., and Hammond R., (2005): Information systems security issues and decisions for small businesses: An empirical examination. Information Management & Computer Security, 13(4), 297-310.
10. Makanju A., Zincir-Heywood A. N., and Milios E. E. (2011).: Robust learning intrusion detection for attacks on wireless networks - Intelligent Data Analysis, 15(5), 801-823.
11. Patel, A., Qassim Q., and Wills C. (2010): A survey of intrusion detection and prevention systems. Information Management & Computer Security, 18(4), 277-290.
12. Puzis, R., Yagil D., Elovici, Y., and Braha, D. (2009). Collaborative attack on internet users' anonymity, Internet Research, 19(1), 60-77.
13. Sevgi O. and Bilge K. (2010): Collaborative risk method for information security management practices - A case context within Turkey, International Journal of Information Management, Volume 30, Issue 6, Pages 567-572.
14. Bonnie C. (2006): Good Governance, Security and Mining in Africa, Pages 31-44.
15. Bajpayee T.S., Rehak T.R., Mowrey G.L. and Ingram D.K. (2004): Blasting Injuries In Surface Mining With Emphasis On Flyrock And Blast Area Security, Journal of Safety Research, ELSEVIER, Volume 35, Issue 1, Pages 47-57.
16. Ninghui L., John C. M. and William H. W. (2005): Beyond proof-of-compliance: security analysis in trust management, *Journal of the ACM, Volume 52, Issue 3*.
17. Chris Y. (2012): The Big Data Opportunity. Policy Exchange. p1-36.
18. Moens S., Aksehirli E. and Goethals B. (2012): Frequent Item set Mining for Big Data, IEEE, p1-8.
19. OndrejVyborn. (2006): Time, Data Mining and Security, Masaryk University, p1-42.
20. SAS (2012): Big data Lessons from the leaders, Economist Intelligence Unit Limited, p1-30.
21. Robert R. (2020): What is Information Security? Definition, Principles, and Policies
22. UsLegal (1997): Personal Security Law and Legal Definition - Mergenthaler v. Commonwealth State Employee' retirement.; www.definitions.uslegals.com
23. Kaspersky (2021): What is cyber security? www.kaspersky.com
24. ASIS (1972): International's Security Management Magazine

APPENDIX/ADDENDUM:

Serial No.	NAME OF DEVICE	PICTURE OF DEVICE
1	Installed CCTV	 (eurovigil.in)
2	Digital Radio of high resolution	 (radiopart.com.au)
3	High Speed Broad Band	 (mainone.net)
4	Video Monitoring Surveillance Security	 (bigstockphoto.com)
5	Biometric Data Security	 (gizbot.com)

6	Barriers	 (Jakachu.com)
7	Turnstile Access	 (esd-turnstile.com)
8	Boom Gates	 (intervid-africa.co.za)
9	RFID Access Control	 (oodak.com)
10	X-ray and Metal Detector	 (foodengineering.com)

11	PTZ Camera