Evaluation and analysis of the Major Security Systems Deployed on Telecommunications Cell Sites

Kwaku Boateng, Isaac Hanson, Owusu Nyarko-Boateng, Amevi Acakpovi

ABSTRACT: Telecommunications companies, also known as Mobile Network Operators (MNO) and tower owners have suffered theft of items on their cell sites ranging from battery backup systems, generator fuel and other valuable items because of lack of proper security systems deployed on their cell sites. This paper examined and evaluated the major security systems deployed on the cell sites, assessed their effectiveness, cost implications of implementation and recommended possible improvements of the security systems. Yamane's finite population formula was used with the purposive sampling technique to achieve a total of 56 responses from questionnaires which were administered to some tower companies and mobile network operator's staff, their subcontractors and onsite security personnel. The data collected was analyzed and interpreted with SPSS and MS excel. The results revealed that telecom cell sites used manned security, abloy locks, electronic locks and very few CCTV security systems sequentially. Some vulnerabilities identified were security persons abdicating their post without any proper handover, thieves destroying palisade fence to access the sites, lack of good visibility of the cell sites by the site field engineers and MNO network operations center (NOCs), etc. It was concluded that security systems deployed have not been beneficial and that theft on cell sites cost tower owners and MNOs several thousands of US dollars. These losses far exceed the cost of security system suggested by majority of respondents to be deployed on the cell sites. Some of the recommendations were, good service level agreement (SLAs) should be signed between the site owners and the security service providers to cater for good work attitude and reporting to the NOCs of security guard'. Competent CCTV professionals should be contracted to install CCTVs that will cover absolute perimeter of the sites. A combination of manned security, electronic locks and CCTVs must be installed at the cell sites because their cumulative cost per year estimated to GHs 13,600 per site, cannot be compared to the GHs 100,000 in radio network availability (RNA) losses per month, as a result of thefts.

Index Terms: Ably padlock, CCTV, Electronic padlock, Cell Site Protection, Theft, Manned Security, and MNOs.

1. Introduction

Security and protection system (Edgar, McInerney & Mele, 1987) according in the Encyclopedia Britannica is defined as any of various means or devices designed to guard persons and property against a broad range of hazards, including crime, fire, accidents, espionage, sabotage, subversion and attack.
Dictionary.cambridge.org also defines security as protection of a building, person, organization or country against threats such as crime or attacks by foreign countries or entities.
A typical Telecom operator's cell site covers an area of about 14sq meters and has various telecom equipment such as Base Transceiver Station (BTS), which is connected to radio frequency antennas via feeder cables (optical fiber or copper coaxial cables) and Microwave transmission systems. The antennas are installed on a mast or tower and the BTS installed on a plinth on the ground in the case of outdoor BTS or in a shelter for indoor BTS sites. The BTS and Transmission equipment are powered by Mains electricity supply (which is converted to a -48volt DC output, whilst for others, the -48vdc is converted to a +24vdc) and backed up by generators and battery bank system.

A cell site equipment can be classified in two main components, the electronic/telecom component also known as the active equipment and the non-electronic component which is also known as the passive equipment. This classification is used to differentiate the team that manages the components as well. Telecom engineers/technicians manage the active equipment whilst the passive units are managed by electrical power/electro-mechanic engineers/technicians. These are illustrated in the Table 1.1.

Table 1.1 Source: Field data, March 2016

Active Equipment	Passive Equipment
Radio Base Station	Shelter
Microwave Transmission equipment	Diesel Generator
Optical Fiber Cables	Generator Tanks

- Author: Project Manager, Active Deployment, M-P Infrastructure, Accra, Ghana
- Co-author: Senior Lecturer, Dept. of Computer Eng., Ghana Telecom University. College, Accra, Ghana
- Co-author: Lecturer, Dept. Computer Science & Informatics, University of Energy and Natural Resources, Sunyani, Ghana
- Co-author: Senior Lecturer, Dept. of Electrical & Electronics Eng, Accra Technical University, Accra,

Antennae	Electric Power system
Coaxial Feeder cables	Tower
Multiplexer unit	SMPS (Switch Mode Power Supply) units and Battery cells

MTNs suffer theft mostly of batteries, cables, fuel, and occasionally generators on their cell sites and these remain one of the major challenges to the operations of the Telecommunications business (Oughton, Frias, Russell, Sicker & Cleevely (2018). The batteries serve as backup in the event of commercial power outage to help maintain telecommunication services until power from backup generators kicks in. Fuel is used to run the backup generators, and the cables are the ones used to transmit network signals from the RBS units to antennas. Because these equipment and materials are prone to theft, the site is normally secured with a gated palisade fence and sometimes security guard or a very good security locking system, and/or electronic security monitoring system are deployed for cell site safety.

These theft activities are mainly carried out by internal and external perpetrators who know the technicalities of the operations and the significance and value of the items (i.e. cables, fuel, batteries) to the network operations.

MNOs have sought to curb these theft activities by deploying various security measures such as

- Security personnel on site either for a 24hr duration with 12hr shift system for day and night, or a 12hr system for only night shift.
- Deployment of security locking system with a universal key, which cannot be duplicated and can open any of the security locks by anyone who gets hold of the key (abloy lock system).
- Deployment of a closed-circuit TV (CCTV) monitoring system, and most recently;
- The deployment of electronic (smart) key locking system that will require that a person whose personal details have been used to request the key is the only one who can get a code to open and close the padlock upon request from the Tower Company's Network Operation Center (NOC).
- The telecom operators also deploy telemetry devices for remote site monitoring and management

With all these security measures deployed, theft has still not stopped.

2.0 Review of Major Security Systems Deployed On Cell Sites

There has not been any published reseach work in this area so the authors had difficulty to have papers to review. The authors used a field data (Field data, 2018) obtained from the perception survey conducted for the literature review.

Security is paramount to the telecommunications industry, but the industry players face unique challenges in implementation because of the way they are structured. Companies must secure their networks while managing hundreds of properties over geographically widespread regions (Hilverda, 2016).

The first type of security deployed after a Network operator builds their site in Ghana is the normal padlock, after which the operator decides which security system to use on site.

MNOs deploy security services to take care of their cell sites similar to any other institution. The types of security deployed includes, assigning a security person to guard the site, use of Abloy lock system which is currently being replaced by electronic lock system. Some have deployed a few closed-circuit television monitoring systems to capture real time movements to and from the site (Sempere, 2011).

2.1 *Security Personnel (Guard) System*

Network operators in Ghana contracted the services of security companies such as Inter-Con, G4S, IForce, Kent house security companies, and others to guard their sites against theft and other hazards such as fire and flood after site build. The security personnel are supposed to guard the site either 24hrs in a 12hr shift (i.e. two guards) or one guard for 12hrs, either during the day or in the night depending on the environment. The personnel are supposed to have a shelter and some basic amenities like washroom near their post.

The guard's duty is to make sure that anyone who enters the site is authorized, he/she logs the persons vehicle number, time of arrival and departure and activity that the person performed. On leaving the site, the visitor to the site signs out and if he/she is taking anything from the site (Field data, 2018).

2.2 *Abloy Padlock and Key System*

Abloy lock usage was adopted in Ghana in year 2008 by MTN Ghana (an MNO) to help protect their cell sites against unauthorized entry, Zain Ghana (now Airtel) also began deploying Abloy locks in year 2011 after suffering from unworthy security guards. The Abloy lock deployment was also as a means of cost saving to the MNOs. The deployment of the Abloy padlock started to substitute security guards in areas where theft was ongoing with suspicion of the guards, and later replaced completely the security guard system. At a point in time the keys to these locks had become so common that any subcontractor of the MNOs had more than one key, which aided theft to increase (Field data, 2018; Biztechafrica, & Reddick, 2015).

2.3 *Electronic (Smart) Padlock and Key System*

A smart lock is an electro-mechanical lock which is designed to perform locking and unlocking operations on a door when it receives such instructions from an authorized device using a wireless protocol. Tower

companies like ATC started to use Acsys smart locking system in 2013 on some of their sites, and other tower companies such as Helios Tower Ghana and Eaton Tower (for Airtel sites) started using smart lock system later in 2013 and early 2014 respectively. The use of this system is supposed to make it possible for the tower companies' NOC to know who accesses the site whenever there is a visitor on site, because the person would require a reference code from NOC to unlock the padlock before access. Conversely, theft has happened on sites with smart locks where the lock was not broken (breaking of lock is highly impossible) but tower company has not been able to provide details of entry (still under investigation), other instances of theft occurred with fence broken to enter (Field data, 2018)

2.4 *CCTV System*

Closed Circuit Television monitoring system (CCTV) is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes. It is a situational measure that enables a locale to be monitored remotely. (Frost & Sullivan, 2007) CCTV relies on strategic placement of cameras, and observation of the camera's input on monitors. Gills and Spriggs, (Matula, 2015), assert that for CCTV, cameras collect images which are transferred to a monitor-recording device, where they are available to be watched, reviewed and/or stored. CCTV is a situational measure that enables a locale to be kept under surveillance remotely. The various types of cameras are; Night Vision camera which uses infrared to illuminate poorly lit area and to record footage at night, the Exterior camera are weather proof and have night vision characteristics, they are normally targeted at entrances. Motion Detection types start recording immediately they sense movement. Thanks to emerging technology, most CCTVs are now wireless, which operate over 3G or LTE technology (Delgado, Silva, Pires & Gaspar, 2017).

But there are indications that CCTV is more effective in sites with limited control access points such as entrance and exits to the target area (Fischer, Halibozek, Walters, 2019).

3.0 Methodology

This research work can be classified as statistical descriptive work as it studies the security types employed by the MNOs operators in Ghana.

Descriptive research define the present condition in more detail and filling in any missing parts to give a clearer understanding (Kowalczyk, 2013). The descriptive aspect investigates the review of present security systems deployed on the various MNOs cell sites and its improvement to suggest a better protection method.

In trying to achieve the objectives of this research, the paper adopted a case study research approach. Case study method for research according to (Yin, 1984), is an empirical examination that investigates a current phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used which involves the use of both qualitative and quantitative methods

Sources of Data

The main source of data for the study was primary data.

Primary Data Sources

The researcher went to the field to collect data considered essential for this research from respondents through the administration of open-ended and closed-ended questionnaires, personal interviews and observations.

Questionnaires were given out to carefully selected respondents. The set of questions were clear and explicit to solicit the right information. The questionnaire was tested carefully before being deployed finally.

MNOs cell sites tower management companies such as Eaton Towers, Helios Towers and ATC who manage most Vodafone, Airtel, Tigo and MTN cell sites in Ghana were contacted for additional information on weaknesses or thefts recorded and the related security system deployed on the telecom cell sites from January 2013 till August 2018.

The related financial losses incurred because of these thefts were also sought to help find out the efficient security system that has been deployed on telecom cell sites in Ghana over the period under study in this research as shown figure 2.

DISCLAIMER: The researcher takes no responsibility of faulty data given to him by MNOs, Tower Owners, or their ASPs

Major Security Systems Deployed on Telecom cell sites

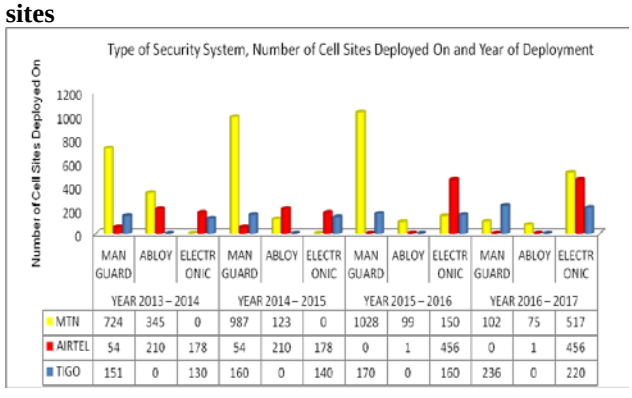

Figure 1 Source: Field Data, January 2013-April 2017 (***No input was received from telecom operator Vodafone for this analysis).***

Review of Major Security Systems Deployed On Telecom Cell Sites

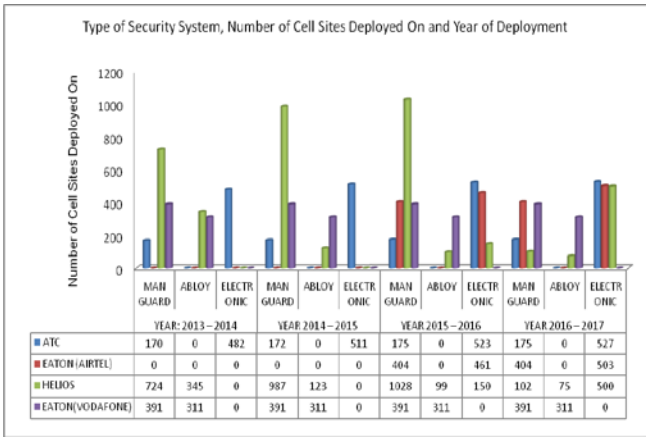

Figure 2 Source: Field Data, April 2017

As indicated in figure 1 and figure 2, ATC which manages most of MTN sites have stopped using Abloy locking system, the same has been with Eaton on Airtel side. MTN and Airtel lost control on management of the Abloy keys to their subcontractors and hence could not track access to their sites (Field data, 2018).
Helios and Vodafone on the other hand maintained the use of Abloy together with man security which they had enough control on. Helios began deploying electronic key in 2016 when they began to have issues with manned security (Field data, 2018).

The Effectiveness of Each Security System deployed on Cell Sites:
In this section, the paper present a review the results obtained from the respondents concerning the effectiveness of all the various security systems deployed on telecom cell sites either.

Manned Security
Manned security involves engaging the services of security personnel either directly or indirectly through a third-party security services provider whose responsibility is to protect the MNO cell site and its contents either on 12-hour or 24-hour basis depending on the terms of engagement. Table 2 represent the results obtained from respondents concerning their views on the efficacy of manned security system and its related challenges.

Was it Expensive to Engage the Services of Security Personnel?

Table 2 Source: Field Data, April 2017

Response	Frequency	Percent
Yes	32	57.1
Partially	18	32.1
No	6	10.7
Total	56	100.0

The results obtained indicates 32 respondents interviewed constituting 57.1% agreed it was expensive to engage the services of security personnel. 18 others representing 32.1% partially agreed while the remaining 6 of them representing 10.7% disagreed that it was expensive to engage the services of security personnel.

Number of Hours Security Personnel Work Daily

Table 3 Source: Field Data, April 2017

Number of Hours	Frequency	Percent
24hrs	28	50.0
12hrs	25	44.6
whenever needed	2	3.6
Total	55	98.2
No Response	1	1.8
Total	56	100.0

From the data obtained as shown in the table 3, 28 (50%) respondents representing half the total number of people respondents' said the security personnel work 24hours daily protecting the cell sites, 25 (44.6%) of them said 12hours while 2 (3.6%) of them also said the services of the security personnel or security companies are engaged whenever the need arose. One respondent did not respond to the question asked.

Frequency of Occurrence of Theft on Cell Sites Manned by Security Personnel

Table 4 Source: Field Data, April 2017

Does Theft Occur on Sites Manned by Security Personnel?	Frequency	Percent
Yes	51	91.1
No	5	8.9
Total	56	100.0

Frequency of Theft Cross tabulation

Table 5 Source: Field Data, April 2017

Does Theft Occur on Sites Manned by Security Personnel?		Frequency of Occurrence of Theft			Total
		Yes	No	Not Always	
Yes	Count	19	30	2	51
	% within Frequency of Theft	37.3 %	58.8 %	3.9%	91.1%

The effectiveness and reliability of a security system will depend on its robustness, efficiency and cost effectiveness in eradicating completely or minimizing possible thefts resulting in losses.

When the respondents were asked if they were aware of occurrence of thefts on telecom cell sites manned by security personnel, 51(91.1%) respondents out of 56 persons interviewed constituting an overwhelming majority confirmed thefts occurred on telecom cell sites manned by security personnel while the remaining 5(8.9%) of them disagreed as shown in table 4.4.1e above. Of the 51(91.1%) respondents who confirmed theft did occur on telecom cell sites manned by security personnel, 19(37.3%) of them agreed the thefts occurred frequently while 30(58.8%) others disagreed and the remaining 2(3.9%) of them agreed the thefts did occur but not always as contained in table 4 and Table 5.

Items Stolen from Sites Manned By Security Personnel

Table 6 Source: Field Data, April 2017

Stolen Item	Frequency	Percent
Fuel and Batteries	40	71.4
Diesel Generator, and Feeder Cable	9	16.1
Batteries	4	7.1
Fuel	3	5.4
Total	56	100.0

In order to know which items were specifically stolen from cell sites manned by security personnel where the respondents confirmed earlier that thefts occurred, the respondents were asked to list the stolen items and the results are shown in table 6.

It can be deduced from the results obtained that 40(71.4%) of the respondent constituting an overwhelming majority stated that fuel and batteries were the items stolen from the cell sites manned by security personnel where they indicated earlier thefts did occur, while 9(16.1%) others said diesel generator and feeder cables, 4(7.1%) of them also mentioned batteries only and the remaining 3(5.4%) of them said fuel only.

Time of the Day Most Thefts Occurred on Cell Sites Manned By Security Personnel

Table 7 Source: Field Data, April 2017

Time of Day Most Thefts Occurred	Frequency	Percent
Late Evenings (10pm – 12am)	17	33.3
Dawn (12am – 5am)	11	21.6
Mornings (6am – 11:59am)	8	15.7
Early Evenings (6pm – 10pm)	7	13.7
At all times of the Day	5	9.8
Afternoons (12pm – 6pm)	3	5.9
Total	51	100.0

It is very important especially for this research to know the exact time of the day when most thefts occurred on cell sites manned by security personnel. In view of this, the respondents were asked to state the specific times of the day when such thefts did occur.

From the data obtained in Table 7, it was observed that out of the 56 persons interviewed, 17(33.3%) of them said most thefts occurred late in the evenings between 10pm to 12pm, 11(21.6%) others said the thefts occurred at dawn between 12am to 5am, while 8(15.7%) of them said the thefts occurred in the morning between 6am to 11:59am, and 7(13.7%) of them said early in the evenings between 6pm to 10pm, 5(9.8%) others said the thefts occurred at any time of the day, and the remaining 3(5.9%) of them indicated most thefts occurred in the afternoons between 12pm to 6pm.

Security Personnel on Duty at Cell Site When Theft Occurs

Table 8 Source: Field Data, April 2017

Was Security Personnel on duty when theft Occurred?	Frequency	Percent
No	44	78.6
Yes	12	21.4
Total	56	100.0

In an attempt to further probe where security personnel were on the day and time the theft occurred, respondents who earlier on said thefts occurred on cell sites manned by security personnel were asked to confirm if indeed the security personnel was on site at the time of the theft event or not. Results obtained are contained in table 8.

From the results sampled, it was observed that 44(78.6%) of the persons interviewed who constitute majority said the security personnel was not on duty, while the remaining 12(21.4%) of them confirmed the security personnel was on duty at the time the theft occurred.

Reasons Identified As Cause for Most Successful Thefts Which Occurred On Cell Sites Manned By Security Personnel

Table 9. Source: Field Data, April 2017

Reasons Identified as Cause of Most Successful Thefts	Frequency	Percent
Security personnel was not at post	43	76.8

Security personnel on duty connived with field technicians or field engineers to steal items on site	5	8.9
Security personnel on duty do not request for cell site access permit from the field technicians or engineers before granting them physical access to the site	4	7.1
Familiarity resulting in friendship between the field technicians or field engineers and the security personnel on duty creates room for negligence and compromises while on duty	3	5.4
Security Personnel Abdicated Post due to nonpayment of his/her salary	1	1.8
Total	56	100.0

Reasons were further sorted from the respondents' as to what could have been the identified causes of most successful thefts that occurred on cell sites manned by security personnel as contained in table above.

From the results obtained in table 9, it was observed that 43(76.8%) of the respondents said the reason for most successful thefts on cell sites were due to the fact that the security personnel were not on duty or at post at the time the thefts occurred while 5(8.9%) of them said the security personnel on duty connived with field technicians or field engineers to steal items on site, 4(7.1%) others said the security personnel on duty did not request for cell site access permit from the field technicians or engineers before granting them physical access to the site which created room for successful theft, 3(5.4%) also said familiarity resulted in friendship between the field technicians or field engineers and the security personnel on duty therefore created room for negligence and compromises while on duty resulting in successful theft

The remaining 1(1.8%) said the security personnel abdicated his post due to non-payment of his salary which made theft of items on the cell site successful.

Did the deployment of Abloy Padlocks on cell sites eradicate or minimize thefts of items on cell sites?

Table 10 Source: Field Data, April 2017

Abloy minimized thefts on Sites?	Frequency	Percent
Yes	46	82.1
No	9	16.1
Partially	1	1.8
Total	56	100.0

Possibility to By-Pass or Breach the Security on Cell Sites Protected with Abloy Padlocks

Table 11 Source: Field Data, April 2017

Possible to Bypass or Breach Abloy Padlock Security?	**Frequency**	**Percent**
Yes	50	89.3
No	6	10.7
Total	56	100.0

Did the deployment of Electronic Padlocks on cell sites eradicate or minimize thefts of items on cell sites?

Table 12 Source: Field Data, April 2017

Electronic Padlocks minimized thefts on Sites?	**Frequency**	**Percent**
Yes	50	89.3
No	3	5.4
Partially	3	5.4
Total	**56**	100.0

Data gathered on respondents view on the effectiveness and robustness of the Electronic padlocks ever since it was deployed on cell sites to replace the Abloy padlocks revealed that 50(89.3%) of persons interviewed who constituted an overwhelming majority were of the firm view that electronic padlocks ever since deployed have minimized theft of items on cell sites while few 3(5.4%) others each either disagreed or partially agreed respectively as shown in tables 10, 11, 12 and 13.

Possibility to By-Pass or Breach the Security on Cell Sites Protected with Electronic Padlocks

Table 13 Source: Field Data, April 2017

Possible to Bypass or Breach Electronic Padlock Security?	**Frequency**	**Percent**
Yes	40	71.4
No	16	28.6
Total	56	100.0

Did the deployment of CCTV Cameras on cell sites eradicate or minimize thefts of items on cell sites?

Table 14 Source: Field Data, April 2017

CCTV Camera System minimized thefts on Sites?	Frequency	Percent
Yes	15	26.8
Not yet deployed	41	73.2
Total	56	100.0

From the data obtained as indicated in table14, it was observed that majority of the persons interviewed confirmed CCTV camera system has not yet been installed on most MNOs cell sites except for Airtel Ghana network which had installed about 10 CCTV cameras for piloting purposes. Hence, the respondents were unable to confirm whether the deployment of CCTV camera system had eradicated completely or minimized thefts of items on cell sites as this research sort to find out.

Estimated Cost Incurred Due to Theft on Cell Sites, Material and /or RNA Losses

Table 15 Source: Field Data, April 2017

In your estimation, how much loss (in material and/or cell unavailability) within the period January 2014 to January 2016 has theft on telecom cell sites cost the company? Please indicate in monetary value	Frequency	Percent
More than $1m	25	44.6
$500,000	10	17.9
$800,000	7	12.5
$200,000	6	10.7
$50,000	6	10.7
Not too sure of the cost of items lost	2	3.6
Total	56	100.0

Cost of Losses on Telecom Cell Sites Due to Theft

From table 15 above, majority of respondents summing up to 42 (75%) agreed that losses generated by cell sites theft between January 2014 and January 2018 are from $500, 000 to more than $1million. The field data above, is also confirming to the fact that MNOs and tower owners suffer very high cost of losses as a result of theft on their cell sites.

4.0 Results and Discussion

This paper assessed the major security systems deployed at the MNOs cell sites in Ghana. The outcome of the research met the specific objectives. The findings from the data collected revealed in figures 2, 3 and 4 revealed that there has been an evolution of the security systems deployed on MNO cell sites from manned security to electronic and few CCTVs deployment. This confirms that, cell site security has evolved from manned security guard at cell sites, to real time remote monitoring (Naicker & Mafaiti, 2019)..

In assessment of the effectiveness of security systems deployed at MNO cell sites, it was found as indicated in tables 2 through to Table 15 that all the major security systems deployed have not achieved their intended purpose, due to various reasons indicated in the various tables by respondents. The major one is that, manned security failed because personnel often left their post without any backup. For the use of abloy padlock, though duplication of the keys was not possible, NOC did not have control of the key users and thieves managed to device other means such as breaking through fence to execute their thievery ambitions. The use of electronic keys gave the NOC enough control of any key user, because they had to give access code before the keys could be used, but again responses revealed that thieves still broke the fence where no visibility was available to site owners. This is what Felson and Clarke asserted in the literature, opportunity calls for crime to be committed (Felson & Clarke, 1998).

Majority of the respondents' indicated that CCTV was not installed on cell sites, though it could provide real time visibility on cell sites to the NOC.

The findings indicated in table 15 that MNOs and site owners incur more than $1 million due to theft on their cell sites that resulted in loss of items and loss of network availability (Purpura, 2019). It was also found as indicated in the data in Table 15 that cell site owners loose thousands of dollars because they do not have good intrusion detection and prevention system on their cell sites.

Respondents also indicated that although it is expensive to deploy a combination of intelligent CCTV system, Electronic padlock and well-trained security person, it would still be cost effective when compared to the losses MNOs and site owners incur because of theft on their cell sites. Thus, when the companies know their needs and are well informed of what to choose, they will know the cost and appreciate it.

Majority of respondent indicated that a combination of manned security system, CCTV and electronic padlock could best protect cell sites. This agrees with Dan Lohrmann's (CSO of Michigan State) assertion when interviewed by Eric Chabrow on the discussion, Taking charge of Physical and IT security in September 2011 (Chabrow & Lohrmann, 2011). In their submission, they said IT and Physical security combination could be the best protection system. Nyarko-Boateng, Asante & Nti (2017) also asserted that it not only physical components that requires protection (Purpura, 2019) but data its related systems must be secured which includes information

transmitted over the web browsers (Appiah, Nti, & Nyarko-Boateng, 2017).

4.1 Conclusion

The outcome of this research has revealed some vulnerabilities in the security systems deployed by MNOs and Tower Owners at their cell sites. Some of which could be listed as: Bad working attitude of the security counterpart and their manned security person on site. This could be attributed to weak SLAs between the two parties Lack of proper visibility on the cell sites which resulted in thieves breaking fence without the NOC having knowledge.
Lack of real time monitoring of activities at the cell sites
Visibility and activity monitoring are not within the control of MNOs and Tower Owners. CCTV with absolute perimeter coverage remote monitoring at the NOC can help eliminate this problem. MNOs and Tower owners have not come to terms with why they should spend on quality security system provision for their cell sites, though they make complains of losses.

REFERENCES

Appiah, V., Nti, I. K., & Nyarko-Boateng, O. (2017) Investigating Websites and Web Application Vulnerabilities: Webmaster's Perspective. International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 12 – No. 3

Chabrow, E. (GovInfoSecurity) and Lohrmann, D. (2011): Taking Charge of Physical, IT Security. Interview available online at https://www.inforisktoday.in/interviews/taking-charge-physical-security-i-1251(Accessed on Dec 23, 2017)

Christopher B. Delgado, Pedro D. Silva, Luís C. Pires, Pedro D. Gaspar (2017). Experimental study and numerical simulation of the interior flow in a telecommunications cabinet, Energy Procedia, Volume 142, Pages 3096-3101, ISSN 1876-6102, https://doi.org/10.1016/j.egypro.2017.12.450.

Edward Oughton, Zoraida Frias, Tom Russell, Douglas Sicker, David D. Cleevely (2018). Towards 5G: Scenario-based assessment of the future supply and demand for mobile telecommunications infrastructure, Technological Forecasting and Social Change, Volume 133, 2018, Pages 141-155, ISSN 0040-1625, https://doi.org/10.1016/j.techfore.2018.03.016.

Felson, M. and Clarke, R.V. (1998) Opportunity Makes the Thief, Practical theory for Crime Prevention. Police Research Series Paper 98, pp 9-13

Field Data (2018). Data collected from the various MNOs and the primary data.

Frost and Sullivan (2007) North American IP Video Surveillance Storage Market N0EA-11 Available online at http://www.emc.co/collateral/analyst-reports/ip-video-surv-storage.pdf (Accessed on December, 2017)

Hilverda, A. (2016) Is Our Telecommunications Infrastructure Secure? Available online at http://www.securityworldmag.com/wsr/wsr_view.asp?idx=1383&part_code=01&page=1 (Accessed on December 15, 2015)

James M. Edgar, William D. McInerney, Joe A. Mele (1987). Key- and Combination-Operated Mechanisms, Editor(s): James M. Edgar, William D. McInerney, Joe A. Mele, The Use of Locks in Physical Crime Prevention, Butterworth-Heinemann, Pages 1-39, ISBN 9780409900927, https://doi.org/10.1016/B978-0-409-90092-7.50006-6.

Jarad Matula (2015). Two Men Charged in 15 Cell Tower Theft. Available online at http://www.rcrwireless.com/20150818/cell-tower-news/two-men-charged-in-15-cell-tower-thefts-tag8 (Accessed on Dec 18, 2015)

Kowalczyk, D. (2013) Purposes of Research: Exploratory, Descriptive & Explanatory. Available online at http://study.com/academy/lesson/purposes-of-research-exploratory-descriptive-explanatory.html. (Accessed on June 16, 2017)

Naicker V., Mafaiti M., (2019). The establishment of collaboration in managing information security through multisourcing, Computers & Security, Volume 80, 2019, Pages 224-237, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2018.10.005.

Nyarko-Boateng, O., Asante, M., & Nti, I. K. (2017). Implementation of Advanced Encryption Standard Algorithm with Key Length of 256 Bits for Preventing Data Loss in an Organization. *International Journal of Science and Engineering Applications*, *6*(03), 88-94.

Neuman, W.L (2007) Social Research Methods: Qualitative and Quantitative Approaches (seventh edition) Pearson New International Edition

Philip P. Purpura (2019). The Business, Careers, and Challenges of Security and Loss Prevention, Editor(s): Philip P. Purpura, Security and Loss Prevention (Seventh Edition), Butterworth-Heinemann, Pages 27-57, ISBN 9780128117958, https://doi.org/10.1016/B978-0-12-811795-8.00002-3.

Robert J. Fischer, Edward P. Halibozek, David C. Walters, (2019) Security: Today and Tomorrow, Editor(s): Robert J. Fischer, Edward P. Halibozek, David C. Walters, Introduction to Security (Tenth Edition), Butterworth-Heinemann, Pages 507-522, ISBN 9780128053102, https://doi.org/10.1016/B978-0-12-805310-2.00020-2.

Sempere, C.M. (2011) A Survey of the European Security Market. Economics of Security Working Paper 43. Available online at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.463.3948&rep=rep1&type=pdf (Accessed on December 17, 2015)]

Yin, R.K (1984) Case Study Research: Design and Methods. Sage Publications, Beverly Hills, California.