NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF ARTS AND SOCIAL SCIENCES

COURSE CODE: CSS 245

COURSE TITLE: PLANNING, DEVELOPMENT AND MANAGEMENT.

COURSE GUIDE

**CSS245
SECURITY PLANNING, DEVELOPMENT AND MANAGEMENT**

Course Team   Mr. Darlington Ikpi (Writer/Developer)
                     Dr. Niyi Adegoke (Coordinator) - NOUN
                     Dr. U.I Adeyinka Aderinto (Editor)
                     Dr. N. Nwabueze (Programme Leader) - NOUN

NATIONAL OPEN UNIVERSITY OF NIGE

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Office
No. 5 Dar es Salaam Street
Off Aminu Kano Crescent
Wuse II, Abuja
Nigeria

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

CONTENTS   PAGE

Introduction

Security Planning, Development and Management

CSS245 is a semester course of 2 credit unit that provides students with the various topics on issues in Security Planning Development and Management. It is prepared for students in the first year of study in Criminology and Security Studies in the National Open University of Nigeria (NOUN).

Security Planning Process is the modern challenges for the study of Risk Analysis, Security Surveys, Financial Planning and Decision making for the development of Security programmes and counter measures of securing the country and maintaining its citizens' rights. This guide provides the students with simple understanding of the role of the Security Manager in the identification, analysis and response to variety of human and natural crisis.

To study this course, and the various units, students need to be ready to think critically. They need to develop constructive minds and use situational analysis, case studies and other research oriented approaches carefully, to buttress arguments in the study of security management situations.

In this course, aims and objectives will be explained. The module provides some useful advice on the reading system, the role in using the course guide, the structure of the module, and guidance for the assessment.

Course Aims

a)   To demonstrate an understanding of the application of security knowledge and techniques to the protection of life and property.
b)   To apply the main theories and concepts of risk analysis and risk management in the security industry.
c)   To outline and critically analyse contemporary issues related to corporate and organisational security asset protection.
d)   To examine the rights guaranteed to individuals by the Nigerian constitution, and how these rights and precedents affect private security personnel.
e)   To critically evaluate and demonstrate the ability to communicate students programmes through a combination of written papers and oral presentations.

Course Objectives

- To introduce students to the concept of security planning, development and management
- To expose students to the various methods for security professionals including the security information technology criteria for purchase, installation and maintenance of computer and networking equipments, including prevention of thefts of data.
- To identify vulnerabilities in federal, state and local infrastructure.
- To acquaint students to be conversant with routine management of security issues and principles of loss prevention, and needs for incident reaction.
- To teach students how to develop an appreciation of potential legal consequences, both criminal and civil, of training and supervision of security management personnel.
- To highlight the major pinpoints salient changes on how the nation and security management must prepare, respond, manage, and mitigate mega-terrorist incidents.

Working through This Course

To complete this Course, students are advised to check the study units, read the recommended books as well as other course materials provided by the NOUN. Each unit contains Self-Assessment Exercise (SAE) and Tutor Marked Assignments (TMAS) for assessment purposes. There will be a written examination at the end of the course. The course should take students about 14 weeks to complete. You will find all the components of the course listed below. Students need to allocate time to each unit to finish the course successfully.

Course Materials

For this course, students will require the following materials:

- the course guide
- study units which are fifteen (15) in all
- textbooks recommended at the end of the units
- assignment file where all the unit assignments are kept
- presentation schedule.

Study Units

There are fifteen (15) study units in this course broken into 3 modules of 5 units each. They are as follows:

Module 1

Unit 1   Introduction and General Background
Unit 2   Planning and Importance of Security Planning
Unit 3   Company Business Interest
Unit 4   Private Security Operation in the Past
Unit 5   Difference between Public and Private Security and their Relationship

Module 2

Unit 1   Design of Security Survey System
Unit 2   The State or National Interest
Unit 3   Operational Duty for Security Staff, Supervisors and Management Functions
Unit 4   Patrol Procedures and Techniques
Unit 5   Loss Prevention and Control

Module 3

Unit 1   Management -Basic Principles of Management
Unit 2   Security Policy and Design
Unit 3   Evaluation of Protection Programme
Unit 4   Administration and Documentation of Security Records and Reports
Unit 5   Samples of Security Procedures for Access Control at the Gate

Each unit contains some exercise on the topic covered, and students will be required to attempt the exercises. These will enable them evaluate their progress as well as reinforce what they have learned so far. The exercise, together with the tutor marked assignments, will help students in achieving the stated learning objectives of the individual units and the course.

Textbooks and References

Students may wish to consult the references and other books suggested at the end of each unit to enhance their knowledge of the material. This will enhance their understanding of the material.

Braimoh, A. (2001). *The Basic Security Knowledge and Planning* U.S.A: New World Press.

Charles, A. S. (1998). *Effective Security Management*. London: Butterworth Heinemann Books Ltd.

David, M (1989). *Private Security Law Case Studies*. London: Butterworth-Heinemann Book Ltd.

Fisher, R. J. & Green, G. (1986). *Introduction to Security Management and Planning*. New York: Paeger Publishers.

Haddow, B & Bullocks. *Introduction to Homeland Security Response and Recovery.* Tokyo: United Nations Press.

Inbau, F. & Arnold, A. (1998). *Protective Security Law* (2nd Ed.). London: Butterworth Heinemann Books Ltd.

Assessment

Assessment for this course is in two parts, Tutor-Marked Assignments, and a written examination. Students will be required to apply the information and knowledge gained from this course in completing their assignments. Students must submit their assignments to their tutor in line with submission deadlines stated in the assignment file. The work that you submit to your tutor for assessment will count for 30% of your total score.

Tutor-Marked Assignments (TMAs)

In this course, you will be required to study fifteen (15) units, and complete tutor-marked assignment provided at the end of each unit.
The assignments carry 10% mark each. The best four of your assignments will constitute 30% of your final mark. At the end of the course, you will be required to write a final examination, which counts for 70% of your final mark.

The assignments for each unit in this course are contained in your assignment file. You may wish to consult other related materials apart from your course material to complete your assignments. When you complete each assignment, send it together with a tutor marked assignment (TMA) form to your Tutor. Ensure that each assignment reaches your tutor on or before the dead line stipulated in the assignment file. If, for any reason you are unable to complete your assignment on time, contact your tutor before the due date, to discuss the possibility of an extension.

Note that extensions will not be granted after the due date for submission unless under exceptional circumstances.

Final Examination and Grading

The final examination for this course will be two hours, and count for 70% of your total mark. The examination will consist of questions, which reflect the information in your course material, exercise, and tutor marked assignments. All aspects of the course will be examined. Use the time between the completion of the last unit and examination to revise the entire course.

You may also find it useful to review your tutor marked assignments before the examination.

Course Marking Scheme

ASSESSMENT	MARKS
Assignments	Four assignments, best three marks of four count at 30% of course marks
Final Examination	70% of total course mark
Total	**100% of course marks.**

Course Overview

Assignment file consists of details of the assignments you are required to submit to your tutor for marking. The marks obtained for these assignments will count towards the final mark you obtain for this course. More information on the assignments can be found in the assignment file.

Course Overview and Presentation Schedule

Unit	Title of Work	Weeks Activity	Assessment (End of Unit)
	Module 1		
1	Introduction and General Background	week 1	
2	Planning and Importance of Security Planning	Week 2	
3	Company Business Interest	Week 3	Assignment 1
4	Private Security Operation in the Past	Week 4	

5	Difference between Public and Private Security and Their Relationship	Week 5	
Module 2			
1	Design of Security Survey System	Week 6	Assignment 2
2	The State or National Interest	Week 7	
3	Operational Duty for Security Staff, Supervisors, and Management Functions	Week 8	
4	Patrol Procedures and Techniques	Week 9	
5	Loss Prevention and Control	Week 10	
Module 3			
1	Management- Basic Principles of Management	Week 11	Assignment 3
2	Security Policy and Design		~~COURSE GUIDE~~
3	Evaluation of Protection Programmes	Week 13	
4	Administration and Documentation of Security Records and Reports	Week 14	
5	Samples of Security procedures for Access Control at the gate	Week 15	Assignment 4
16	Revision	Week 16	
17	Examinations	Week 17	
	Total	**17 Weeks**	

How to Get the Most from This Course

In distance learning, your course material replaces the lecturer.

The course material has been designed in such a way that you can study on your own with little or no assistance at all. This allows you to work, and study at your place, and at a time and place that best suits you. Think of reading your course material in the same way as listening to the lecturer. However, you are advised to study with your course material in the same way a lecturer might give you some reading to do. The study units give you information on what to read, and these form your text materials. You are provided exercise to do at appropriate points, just as a lecturer might give you an in-class exercise.

Each of the study units follows a common format. The first item is an introduction to the unit, and how a particular unit is integrated with the other units and the course as a whole. Next to this, is a set of learning objectives. These objectives let you know what you are required to learn by the time you have completed the unit. These learning objectives are meant to guide your study. The moment a unit is finished, you must go back and check whether you have achieved the objectives. If you make

this a habit, it will improve your chances of passing the course significantly.

The main body of the unit guides you through the required reading from other sources. This will usually be either from the reference books or from a reading section. The following is a practical strategy for working through the course. If you run into difficulties, telephone your tutor. Remember that your tutor's job is to help you when you need assistance, do not hesitate to call and ask your tutor for help or visit the study centre.

Read this Course Guide thoroughly is your first assignment.

1)   Organise a study Schedule, Design a "Course Overview" to guide you through the course. Note the time you are expected to support on each unit and how the assignments relate to this unit. You need to gather all the information into one place, such as your diary or a wall calendar. Whatever method you choose to use, you should decide and write in your own dates and schedule of work for each unit.

2)   Once you have created your own study schedule, do everything to be faithful to it. The major reason students fail is that they get behind with their course work. If you get into difficulties with your schedule, please, let your tutor know before it is too late for help.

3)   Turn to unit 1, and read the introduction and the objectives for the unit.

4)   Assemble the study materials. You will need the reference books in the unit you are studying at any point in time.

5)   Work through the unit. As you work through the unit, you will know what sources to consult for further information.

6)   Before the relevant due dates (about 4 weeks before due dates), access the Assignment file. Keep in mind that you will learn a lot by doing the assignment carefully, they have been designed to help you meet the objectives of the course and pass the examination. Submit all assignments not later than the due date.

7)   Review the objectives for each study unit to confirm that you have achieved them. If you feel unsure about any of the objectives, review the study materials or consult your tutor.

8)   When you are confident that you have achieved a unit's objectives, you can start on the next unit. Proceed unit by unit through the course and try to pace your study so that you keep your self on schedule.

9)   When you have submitted an assignment to your tutor for marking, do not wait for marking before starting on the next unit. Keep to your schedule. When the Assignment is returned, pay

particular attention to your tutor's comments, both on the tutor-marked assignment form and also the written comments on the ordinary assignments.

10)   After completing the last unit, review the course and prepare yourself for the final examination. Check that you have achieved the unit objectives (listed at the beginning of each unit) and the course objectives (listed in the Course Guide)

Facilitators/Tutors and Tutorials

There are 15 hours of tutorials provided to support this course. Tutorials are for problem solving and they are optional. You need to get in touch with your tutor to arrange date and time for tutorials if needed. Your tutor will mark and comment on your assignments, keep a close watch on your progress and on any difficulties you might encounter and provide assistance to you during the course. You must submit your tutor-marked assignments to your tutor well before the due date (at least two working days are required). They will be marked by your tutor and returned to you as soon as possible.

Do not hesitate to contact your tutor by telephone, e-mail, or discussion board. The following might be circumstances in which you will find contacting your tutor necessary.

- You do not understand any part of the study units or the designed readings.
- You have difficulties with the exercises.
- You have a question or problem with an assignment, with your tutor's comments on an assignment or with the grading of an assignment.

To gain maximum benefits from this course tutorials, prepare a question list before attending them. You will learn quite a lot from participating in the discussions.

Summary

The course guide has introduced you to what to expect in Security planning, development and management. It examines the general background of Security Planning and importance of Security Planning, differences between public and private security and their relationship, operational duty for security staff supervisors and management functions, loss prevention and control.

The course also discusses the security policy and design, basic principles of management, administration and documentation of security records

and reports and samples of security procedures for Access Control at the gate. Upon completion you should be equipped with the foundation for analysing and researching security planning and security management issues.

We wish you success with the course and hope you will find it engaging, practical and rewarding.

Course Code   CSS245
Course Title   Security Planning, Development and Management

Course Team   Mr. Darlington Ikpi (Writer/Developer)
                     Dr. Niyi Adegoke (Coordinator) - NOUN
                     Dr. U.I Adeyinka Aderinto (Editor)
                     Dr. N. Nwabueze (Programme Leader) - NOUN

NATIONAL OPEN UNIVERSITY OF NIGERI

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Office
No. 5 Dar es Salaam Street
Off Aminu Kano Crescent
Wuse II, Abuja
Nigeria

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

CONTENTS   PAGE

MODULE 1

UNIT 1   INTRODUCTION AND GENERAL BACKGROUND

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Content
        3.1   Definition of Industrial Security
                3.1.1   Historical Background to Security Management
                3.1.2   The Industrial Revolution
                3.1.3   The Rise of the Industrial Security in Nigeria
3.2   Impact of Loss
3.3   Corporate Terrorism
4.0   Conclusion
5.0   Summary
6.0   Tutor-Marked Assignment
7.0   References/Further Reading

1.0   INTRODUCTION

A way of understanding any subject is to know its definition, the history behind the concept, its nature, purpose and scope. To understand industrial security, we must define what it is, and the definition should be in such a way that it would be meaningful to all.

2.0   OBJECTIVES

At the end of this unit, you should be able to:

- state whose responsibility is Industrial Security
- identify advantages of Security Set Up
- state the disadvantages of not having one.

3.0   MAIN CONTENT

3.1   Definition

Industrial Security management can be defined from various perspectives depending on whom and what is actually involved. Generally, it is regarded as deliberate activities to satisfy the need, to ensure the absence of danger and wary, and to prevent unacceptable loss and danger to corporate assets (tangible and intangible), so as to enhance business profitability. In this sense, industrial security entails awareness, avoidance, planning, protection, preservation, alarm, deterrence and reaction.

3.1.1 Historical Background to Security Management

Although the systematic study of security management as a separate branch of human knowledge has a recent origin, the practice of security management is as old as human society.

The story of security dates back through thousands of years in human history when individuals, communities and groups recognised the threat, danger or peril around their lives and property, and made efforts, individually and collectively to   protect their lives and property. The philosophy of security is embedded in an age-long ideology that was from creation and God sanctioned our lives by nature for protection. Adam was securing Garden of Eden before he misbehaved and was sent away by God.

The history of man is replete with activities which led to emergence of the idea that is now known as security management. Archeology has unearthed extensive accumulations of elaborate security achievements. The mammoth worlds of the ancient Babylon, the pyramids of Pharaohs, the Roman Empire, etc. rival the accomplishment of modern security management considering the state of technology.

The glory that was Rome must be credited in great part to superior activities. Roman region conquered an empire that in the 2nd century of the Christian era, comprehended the farthest past of the earth and the most civilized portion of mankind. 'These vast domains were linked together by an elaborate security network that started from Rome into the other provinces.

3.1.2   The Industrial Revolution

A lot of history, economics and other business books have been filled with accounts of the technological innovations of the industrial revolution in Great Britain and United States of America. Little was know about the security management methods and techniques that helped to make that progress possible. It seems highly unlikely that they could have made the industrial progress of the 19th century without a foundation of successful security management.

The advent of the factory as the primary mode of production, and the tremendous rise in the volume of production of industrial revolution also created a need for large number of security managers.

The factory system may be distinguished from other modes of production in that workers, stocks of raw material and finished goods, machines and equipment, documents and other assets were concentrated in one building or group of buildings. It also brought centralised control of production between the employer and the employee.

The industrial revolution was a major contributory factor in the rapid development of the factory system, furnishing both the power and the machines for large-scale production, and large amount of capital were required to finance the factories.

Since the crafts worker lacked the resources to buy the machine or to compete with machines, he assumed the role of an employee and the bourgeois class who had the money to assume the role of employer. The relationship between the employer and the employee become impersonal.

As a result of the impersonal relationship between the employer and the employee, the latter felt that he was no longer an organic part of the organisation and his interest in the organisation as a whole rested in its ability to pay him a wage with which he nurtured his body and soul.

The industrial revolution also made affluence possible, caused in income disparity, and displaced the crafts worker who cannot complete with machines. The new challenges, frustrations and temptation aggravated offences of physical need and criminality of affluence and, greed.

Another contributory factor is the capitalist system, wherein the bulk of goods and services needed by society are created and distributed by private enterprise in search of profit, with its essential attributes of materialism, private property, free enterprise, profit motive, self interest, competition and the price mechanism. People became preoccupied with

material possession- the rich were respected for their wealth whiles the poor were disrespected for their poverty.

Consequently, most people wanted to become rich and be respected. Many people engaged in different types of activities, such as manufacturing, banking, office work, robbery, pilferage, kidnapping, assassination, dope selling, pimping, etc. in order to get rich.

SELF-ASSESSMENT EXERCISE 1

Why did the relationship between the employer and the employee become impersonal?

3.1.3   The Rise of the Industrial Security Class in Nigeria

Some thirty years ago very little was known about the industrial security career in Nigeria. Only very few Government agencies and parastatals had security departments. They included the Central Bank of Nigeria, the Nigeria Security Printing and Minting Company, the Universities and in later years the Nigeria Ports Authority and the Nigeria Airport Authority. The security department of the Nigeria Ports Authority did not last very long. It was dissolved for undisclosed reasons.

The only known security agency was the Nigeria Police, which was Government's sole legally constituted agency for crime prevention and law enforcement. Also the Armed Forces for safeguarding the security of the country from overt outside aggression.

As the economy of the country progressed, especially with the enactment of the Nigeria Enterprise Promotion Act of 1972 and 1977 (otherwise known as the Indigenisation Decree), many business which were hitherto in the hands of foreign businessmen passed into the hands of Nigerians. There was sudden upsurge in government revenue from petroleum exploration, the economy became suddenly over liquid. The result of the excess liquidation was inflation.

Three major problems that immediately faced the emergent Nigerian entrepreneur include the problem of how to organise his newly acquired business to avoid disruption and possible collapse that the unplanned change in management may cause,.How to cope with the run-away inflation which had badly eroded the purchasing power of the naira, and how to contain the increasing offences of physical need and the criminality of greed from within and without the enterprise so as to enhance profitability. The worsened general economic conditions soon after the Nigerian civil war, coupled with lack of necessary goods, the

realisation of extreme sacrifice, and the spreading disappointment and discontent caused insecurity of life and property to rise threateningly.

The post war period was characterised by increase in offenses of physical need, above all, theft, pilferage, and fraud, falsehood, and so on perpetrated by demoralised youths, women and members of the more educated class. Added to this was a frightening lack of necessary goods and also jobs, and finally a general shortage of money as well as increased number of orphaned and illegitimate children worsened the situation.

Under the above circumstances, it is not surprising that in the postwar era the Nigeria Police could not provide the much needed security cover to individuals and corporate organisations.

More so, as the growing affluence manifested itself in an increase of the criminality of greed, crime changed its forms of appearance and adapted itself to the emerging new technology and economic conditions. Wealthy individuals and corporate assets became more exposed to security risk. Companies continued to record colossal increase in loss. The need for trained security experts tripled. But adequate manpower was not just available.
Ex -policemen and Ex-servicemen were not willing to return to the office for redeployment because work then was regarded as slavery. They saw it as something that was confined to the gate or patrol.

At the end of the Civil War in 1970, many policemen and soldiers who were not reabsorbed into the Police Force and the Armed Forces were desirous of accepting the job of security. This marked a turning point, as the arrival of knowledgeable men in the industrial security scene / career, made a world of difference. A new lease of life was injected into various aspects of industrial security.

Many organisations have full time security departments, comprising of well educated and trained personnel, and with competitive salaries and remunerations like their counterparts in other professions, with the prospects of advancing to chief executive officers (CEOS) position. Industrial security is a profession worldwide today.

3.2   Impact of Loss

To further appreciate the importance of industrial security let us consider the impact of business loss on the consumer.

Example 1

XY Ltd. Produced 50,000 units of a product at N5.00 each. At the warehouse it was discovered that 10,000 units have been stolen. What effect will this theft have on cost and price assuming that a 20 percent return on investment is the profit expected, and XY Ltd incurred about N16, 000 as storage, transportation, selling and other expenses to sell the remaining goods. At what price must XY Ltd sell to make its 20 percent return on investment?

Cost & unit selling price:
A. Without theft:

Production cost - 50,000 at N5 each	=	250,000
Excise Duty 10% of cost	=	25,000
All other expenses (40k per unit)	=	20,000
	=	295,000
Add 20% profit margin	=	**59,000**
Total cost-plus profit	=	354,000
Unit selling price	=	N7.08

B.   With theft:

Production cost (40,000 + 10,000) *	=	250,000
Excise Duty 10% of N200, 000	=	20,000
All other expenses	=	**16,000**
		286,000
Add 20% profit Margin	=	57,200
Total Cost plus Profit	=	**343,200**
Unit Selling Price	=	N8.58

From the above, it can be seen that while each product ought to have been sold for N7.08 if there had been no theft-, with the theft, each had to be sold for N8.58 producing an increase of Nl.50 in unit selling price. In all, the consumers have to be dispossessed of N60, 000.00 because of this loss. The loss leads to inflation of consumer price- downsizing (where the producer absorbs all the cost increase occasioned by the loss)-, increased criminal activities, general insecurity etc.

In general, three possibilities exist:

- the consumer pays for all the cost increase resulting from the loss.
- the consumer and producer share the cost increase resulting from the loss
- the producer absorbs all the cost increase resulting from the loss.

Example 2:

A cell phone was reported missing in the Administrative Department of ABC Nigeria Limited.

ACTION	TIME	COST
Office staff stop work for 15 minutes to help search for the cell phone	6 x 15 minutes	N 150
Supervisor takes details from victim and reports incidents to security	2 x 15 minutes	N 150
Security Department responds and takes statement	2 x 45 minutes	N 150
Security officer's report passed by Supervisor to security Manager to investigate	2 x 1 hour	N 150
Exit Searches	2 x 1 hour	N 200
Suspect apprehended, interviewed, supervisor and police called	3 x 2 hour	N 600
Total	**=**	**N 1, 400**

From the foregoing already N1, 400.00 has been lost in terms of time. An official investigation will then follow during which the Police will interrupt the work of the office to take witness statement. If the decision is taken to prosecute, witness will be required to attend court. The suspect if found guilty will be terminated. The total cost is likely to exceed the sum of N20 000.00 this is why insecurity prevention is better than detection

Another Example:

Micro Computer Services Ltd is a one -stop supplier of IT services to local business, employing 15 staff. It supplies and installs computers and peripherals, provides web hosting services and provides back-up facilities for sensitive company data. The company is housed in a small multi-occupancy office building on the outskirts of Port Harcourt.

Last night, after work, a fire broke out in one of the computers. Fire alarms were activated and the fire service alerted, but by the time they had arrived, ten minutes later, the room in which the computer was housed was ablaze

It took fire fighters several hours to extinguish the fire. Initial estimates put the damages at N50, 000,000.00. The company does have insurance but the suite of offices has been extensively damaged and will be unusable for sometime.

The consequential losses resulting from such event could be catastrophic for the business, and are likely to include many of the following-

- Loss of operations (profit-generating activities)
- Loss of profits
- Investigation cost
- Salaries to staff not working
- Loss of customers
- Customers' losses
- Litigation
- Loss of credit worthiness
- Increase in insurance premiums

SELF-ASSESSMENT EXERCISE 2

Discuss why insecurity prevention is better than detection

- Insurance claim loss adjustment
- Rehiring of staff
- Retraining of staff
- Cost of temporary accommodation and equipment
- Replacement of fire equipment
- Rebuilding and reprogramming of IT systems
- Recreation of data
- Collateral damage to neighbours
- Payment to distribution staff
- Preventative maintenance
- Re – cleaning
- Redecorating
- Restoration of communications
- Loss of image
- Perished raw materials
- Perished finished goods
- Loss of market share
- Advertising following back to normal
- Cash flow problems
- HSE inspections before resumption of activity
- Loss of suppliers if dependent
- Need to buy in services at higher price to support maintenance of market share.

3.3   Corporate Terrorism

Corporate terrorism is a breach of corporate security. It is a threat to corporate live and property. It also exposes the handicap and inefficiency of the company's intelligence security. The overwhelming temptation is to sweep the handicap and inefficiency under the rug or nail management on the cross of security incompetence. It is noteworthy that, intelligence security is within the realm of the security department's function. The security department must feed management with enough intelligence information. Perhaps, this may call for the creation of intelligence section within the security department. Some companies in Nigeria call this section 'spy'.

The security network's red - alert message should help management to burst corporate terrorists and industrial espionage bid in the buds. A security manager that is worth his salt must initiate action for the collection, coordination and communication of intelligence information on the activities of violent and / or potential violent employees. He must develop a network with undercover operatives to cultivate information about sources of terrorist' gangs, and assemble, analyse, assess, and communicate security intelligence (about threats and or potential threats to the company's rights) to management.

The management may refuse to believe the intelligence information as did Director X when in mid - July 1999 the security manager radioed him of a planned invasion of the company's industrial area by youths from the community, on Monday, August 9. He expressed surprise and regretted his -disbelief when the attack did take place on the date the security manager predicted. More than 2,000 rioters from the community invaded the company premises, burning houses and looting company property.

The police were alerted. They arrived and in panic, they shot into the crowd resulting in the death of the rioters. This sparked off another round of destruction as the youths broke through the police barrier and headed down the police station, sacked and set it ablaze

On the other hand, the management may believe the intelligence information, as did Director A, when the company security intelligence confirmed planned hostage taking of its staff by youths from the Area. Director A immediately summoned the community representatives including elders, youth's leaders and women leaders for dialogue, government representative presiding. And an agreement was reached on ways of resolving the issues raised by the community. A replica of ugly situation was averted with understanding reached and cooperation guaranteed.

Information seen to be unimportant may soon develop, that what was communicated was merely the tip of the iceberg. Hidden beneath the business environment lay a monstrous destructive force, that could threaten to rip the bottom right out of the ship of commerce and industry.

4.0   CONCLUSION

In this unit, we highlighted the definitions and concepts of industrial security. We traced the history of security to the mammoth worlds of the ancient Babylon, the Pyramids of the Pharaohs, the Roman Empire etc. We also discussed the contribution of the industrial revolution to industrial security, the rise of industry security class in Nigeria and impacts of loss on the consumer, the company and the society at large.

5.0   SUMMARY

In this unit we have come to know that industrial security is necessary to avoid ugly situation. The purpose of any business enterprise is to enhance profitability by providing safeguard against losses that would have been caused by waste, accident, error and crime, including under utilisation of man-hours.

6.0   TUTOR- MARKED ASSIGNMENT

1.   Define Industrial Security.
2.   Mention various factors that contributed to industrial revolution.
3.   Describe three major problems of the rise of industrial security.
4.   Explain possibilities of reactive measures to impact of loss.

7.0   REFERENCES/FURTHER READING

Revolutionary Pressure in Africa (RPA) (1981). Political Economy of Africa.

Fisher, R.J. & Green, G. (1986). *Introduction to Security Management and Planning*. New York: Paeger Publishers.

Haddow, B. & Bullocks, H. (2000). Introduction to Homeland Security: *Historic Overview of the Terrorist Threat*, (Ed.) Tokyo: United Nations University Press.

UNIT 2   PLANNING AND IMPORTANCE OF SECURITY PLANNING

CONTENTS

1.0   INTRODUCTION

It is a common mistake to put the cart before the horse in security planning, that is, to create a department, hire personnel, and then look around for something to do in a corrupt working environment. Losses almost certainly, exist, and something therefore must be done about them.

2.0   OBJECTIVES

At the end of this unit, you should be able to:

- state when to establish crime prevention unit
- state detailed analysis of potential area of loss
- identify probability and gravity in terms of loss for cooperate goals
- identify steps in the planning process.

3.0 MAIN CONTENT

3.1 What is Security Planning?

Security planning can be described as a process of establishing objectives, allocating resources within prescribed or authorised budgetary limitations, and determining what should be done, how it should be done, and how soon it should be set into operation. It is the security manager's responsibility to determine what the security objectives should be, what the goals in each area of objectives should be. He decides what has to be done. Reach the objective that is definition of ends, and the determination of appropriate means of achieving the desired ends. He decides on who should do what; how it should be done; when to do it and where to do it. Consequently, this aspect of his job involves hard thinking since it is future oriented. Security planning, in the main, requires specificity and purposefulness. Most importantly, the process of planning involves establishment of standards (against which actual performance will be compared), thus, the importance of control to prevent deviation, developing rules, regulations and standard operating procedures, developing the **road map** which will help the security manager to decide for one or more specific course of action. For example, if a company's objective is higher profits and the widespread prevalence of employee theft is eating away those profits, a primary objective of the security function should be to reduce employee theft, and thus contribute to the corporate objective of increased profits.

Importance of Security Planning

Security Planning must include the following.

a.   Specify what is to be achieved
b.   Provide direction
c.   Help translate opportunity into selected course of action
d.   Enhance efficiency and effectiveness
e.   Help conserve valuable resource
f.   Provide for orderly change and continuity
g.   Enhance personnel morale
h.   Reduce crises in the company.

It is important to stress here that planning provides direction and a sense of purpose of the security. The point had earlier been made that security plans are loss prevention road maps. Through planning the loss prevention function keep adapted to its dynamic environment. A good security plan must be able to reveal' potential threats. Even though security plan cannot completely eliminate the risk of loss, yet it can help

identify potential threats and at least minimize loss. A good security plan should be able to specify what is to be achieved. This will be the basis upon which security performance will be measured and controlled.

3.1.2 Steps in the Planning Process

The planning process involves several steps.

1. The definition of a company's central concept.
2. What business is the company into; its product or service and the corporate competitive advantage (if any). In addition this definition will enhance the following.

- Need to recognise causes not symptoms
- Need to know and understand how situations have arisen
- Need to recognise what the company should be and must
- do as basis for deciding alternative causes of action.

3.1.3 Establish Goals

There are goals the security function will pursue. The goals or objectives must be such that can be accomplished. This will provide the standard against which actual performance is measured and compared. The goals must be SMART: specific, measurable, achievable, realistic and time bound.

3.1.4 Develop Forecasts

This is an estimate or prediction of the future status and patterns of crime. It is aimed at calculating or predicting days or seasons on which problems occur; targets for crime, profile of the type and incidence of crimes, patterns of crime and its **modus operandi**, and predictable shape or description of criminal assaults on company property-assists.

These are the premises upon which a security plan is built. Despite the shortcomings of forecasting, yet it is generally more useful for security managers to consciously forecast and develop explicit planning assumptions. Risk analysis and security survey are pre-requisite to good security planning.

3.1.5 Evaluation of Resources

It is important to carefully assess fund availability, managerial and operating resources in order to determine what exactly is or is not feasible. Further, it is important here to analyse relevant facts such as: who will be affected by these problems? What will be their views and

problems? Has someone else experienced this problem? Where possible could relevant information on the problem be obtained?   Who can supply it? These are all relevant questions. They need answers too.

SELF-ASSESSMENT EXERCISE

Briefly analyse the importance of security planning.

3.2   Develop Alternatives

It is sure that several alternatives - individual courses of action that will allow for accomplishing of goals will surface, after a planner must have made the necessary threat assessment and after the careful auditing of one's resources. What is important here is the existence of some choice- which is usually a prerequisite for effective decision -making.

3.3   Tests for Consistency

At this point various alternatives are compared with available resources, goals and central concept of the company. An important point here is that the security function must choose an alternative that is not only in line with the corporate goals and concept, but that which it can easily achieve.

3.4   Deciding on Plan

This is the stage when a choice is made from among the available alternatives. This is of vital importance because where a poor decision (of a very good plan) is made, and thus a wrong "road" is taken - none but the luckiest survive when, and if, it happens. This is one good reason why it is important to analyse and weigh consequences of any security decision. Find out the following.

- What are likely obstacles to implementing the plan?
- How can the problems be avoided or overcome?
- Who is vital in the plan that need be consulted?
- What time is needed?

3.5   Implementation of the Plan

Planning (no matter how effective) is not a guarantee of success. This is because success depends on the effective implementation of the plan. This requires all good skills learnt in organising, investigating, etc. to ensure implementation of decision.   Therefore, one needs to set up budget or schedule of actions, and then assign responsibilities to subordinates.   It is important to check responsibilities and where

necessary one should modify, which is why, from the onset one's plan should be flexible.

3.6   Evaluations and Revision of the Plan

At this stage security plans are periodically evaluated and modified to meet constant changes in the society or environment.

4.0   CONCLUSION

Security planning, including risk analysis and security survey will result in a determination of the degree of security required in all areas of a company. Decisions must also be made as to the means by which such security can be most efficiently, effectively, and economically achieved. New policies and procedures may be ordered, and the size and deployment of security personnel will be determined. All of these factors must be balanced in the consideration of the protection of the company/facility to arrive at a formula providing the most protection at the least expense.

The essential elements of any security control system are as follows.

a)   A predetermined standard (plan, goal, objective, policy, procedure etc.)
b)   A measurement of actual performance.
c)   Comparison of the actual with standard. Results in a variance or a deviance; and
d)   Correction/revision (if necessary)

Control must be instituted over procedures such as transportation, receiving and warehousing, inventory, cash handling, auditing, accounting, staffing and so forth. Since all of these functions are performed in other departments, the most efficient and effective method of implementing such controls is by the presentation of an accountability system to the department manager, allowing him to express his views and make counter-suggestions. There is no reason to support that a totally satisfactory control procedure cannot be reached in this spirit of mutuality.

Only when such controls breakdown or prove to be inadequate should the security manager or his deputy step in to handle the matter directly. Loss preventive controls also cover all physical protection devices, including internal and external barriers of all kinds, alarm and surveillance systems, and communication systems. Identification and traffic patterns are other necessary controls. Identification implies the recognition of authorised versus unauthorised personnel, and traffic in

this context includes all movement of personnel, visitors, vehicles, goods and materials

5.0   SUMMARY

It has been suggested that the following factors should be considered in setting up a company's security system.

- Corporate goals and objectives
- Cost effectiveness of technology/ basic security systems
- Fund availability
- System efficiency through impact of security personnel
- Performance monitoring.

6.0   TUTOR-MARKED ASSIGNMENT

1. Analyse the relevant facts in the course of Evaluating Resources.
2. What are the steps required for the security planning process?
3. Mention few Establishments of Security goals.

7.0   REFERENCES/FURTHER READING

Braimoh, A. (2001). *The Basic of Security Knowledge*. U.S.A: New World Press.

Charles, A.S. (1998). *Effective Security Management* (3rd Ed). London: Butterworth Heinemann Books Ltd.

UNIT 3   COMPANY BUSINESS INTEREST

CONTENTS

1.0   INTRODUCTION

Before delving into the study of the business of security, it is important to describe a company, an entity which warrants industrial security.

We are all aware of the devastating effect of depression in Nigeria's economy. To leave the future of the surviving companies with little or no attention as to the security of their assets could be more devastating.

History attests to the major role companies play in the economic and social development of nations and, the prosperity of companies means the prosperity of the investing public. Company's assets remain the measure of its strength. A weak resource base must affect a company's performance and the implementation of its objectives, goals and operational policies.

2.0   OBJECTIVES

At the end of this unit, you should be able to:

- state the rights to carry out its activities as defined in its co
- state the rights to acquire and hold property in its name for the purpose of its business (es)
- state the rights to sue and be sued
- state the rights not to be discriminated against etc
- state the rights to protest its assets. (Section 289-293, of criminal code Act. CAP 77 LFN 1990).

3.0   MAIN CONTENT

3.1   What is Company?

Company means persons associating for economic gains and profits. The legal frameworks for company matters in Nigeria are detailed in the Companies and Allied Matter Decree No. 1 of 1990. Registered companies are legally recognised as corporate persons who can acquire assets and hold properties in their own names.

As do natural persons, companies as corporate citizens are entitled to security of their assets. As an artificial person in the eye of the law, an incorporated company is entitled to all the rights, which are available to natural persons of full legal capacity.

3.1.1   The Concept of Company

The foregoing shows that the law places collateral responsibilities in the form of certain obligation and duties to companies. These include the duties to respect and promote human rights and fundamental freedom, in all spheres of their activities,. Also to observe all laws and orders made by the State for peace and order. Discharge tax and other financial responsibilities and duties, including social responsibilities under the

national environmental standard with particular reference to land, water, air, noise level, hazardous substance and public health etc. Companies like natural persons are entitled under the law to all rights and protection of the general laws with reference to its assets, be it real, personnel tangible or intangible, including patent, goodwill, etc.

Forms and Types

An increasing number of people, organisations, agencies and interest groups are more concerned with the security industry. They are no longer content with taking a back seat when matters concerning the security industry come into focus. These increased concern and public participation are largely due to the general awareness, resulting from the impact produced by the sector on the national economy and people.

In the provision of security services, there are four key players. These are the Government, Security Agencies, Citizenry and Judiciary.

3.2.1 Government

The chapter two of the 1999 Constitution states clearly that the objective of Government (at all levels) is the security of lives and property of citizens and their welfare. Company is one of the citizens.

3.2.2 Security Agencies

These include the Nigerian Police, Armed Forces, Fire Service, Prison service, Customs, Immigration, and other law enforcement agencies, and private security companies who provide additional security services.

3.2.3 Citizenry

It is the responsibility of the citizens to assist Government and Security by providing relevant information, and tip-off, for effective protection of lives and property.

3.2.4 Judiciary

These include the Customary Courts, District Courts, Magistrates Courts, High Courts, Court of Appeal and Supreme Court. Each of these should be explained briefly.

SELF-ASSESSMENT EXERCISE 1

Explain the four key players of security industry.

3.3   Services and specialties

The security industry could be broadly divided into two: the public and private security organisations that provide protective and safe measures for a continuously expanding landscape of potential vulnerabilities.

The industry operators in Nigeria include the police, Armed Forces, Prison Services, Customs, Immigration, other law enforcement agencies and private security companies, with supporting and complimentary roles.

3.3.1 Proprietary Security Services

The security departments of most public and private companies are manned by professional industrial security managers and operatives. The company tells the employee what to do and how to do it. Their job is done as part of the company and not just for the company. More so, they are treated as employees of the company.

3.3.2 Contract Security Services

Means the supply of security manpower, security Equipment, etc. to individuals, companies, institutions, and establishments as and when required for protection of lives and property, and prevention of loss on contract or hire basis.

3.3.3   Security Consultancy

Many organisations make use of the security consultants; provide specialised security consultancy services and   advice,   professional security education, security system audits, design/engineering of security, fire prevention, and executive protection, etc. They work alone or in partnership for professional fees.

3.3.3   Security Equipment Manufacture, Sales and Services

 This is the manufacture, wholesale, distribution, installation, etc. of security equipment and gadgets ranging from burglar and alarm system- safe- intelligence self defense mechanism, CCTV movement detectors devices for preventing and detecting intrusion, of premises, interference with property- and fire and smoke detectors; bomb and metal detectors etc.

These opportunities can further be categorised according to specialty as follows: Guard security, security consulting, executive protection, security Architecture and design, workplace violence, Background

Investigation, Academic programmes, Anti-terrorism, Engineering Security, Computer Security, coupon fraud, Emergency/Disaster Management, Employee Theft, Facility, Management, Fire prevention, Human Resources, Information Security, Security system Audits, Law Enforcement Management, Liability/Legal Aspects of Security, Office/Multi-Residence Buildings, Physical Security/Access control, safety management, sales/services of security Equipment, Security/ Criminal Justice Education, security force management, security personnel, investigation and polygraph, detective, white collar crime, Alarm dealer security service, etc. The professional industrial security practitioner is to apply intelligently the systems, which are available to him to cope with the increasing challenges of the complex dynamic 21st century technology, and the high expectations from the management and workforce.

3.3.4 The Roles of Industrial Security

The roles of industrial security are as follows.

1. The prevention of loss of company assets crime.
2. The protection of company assets from fire, fraud, damage and trespass.
3. The preservation of company rules and regulations.
4. The maintenance of company prestige at all times.
5. The protection of company personnel from fire, accident and other hazards.
6. The detection of offenders if crime is committed.

3.4 Problem of the Security Industry

There are many problems militating against industrial security in Nigeria. These include-.

3.4.1 Environments

The constraints against industrial security start from the environment, which are not enabling. The socioeconomic and political climate has not encouraged industrial security. Inclusive is widespread security unconsciousness.

3.4.2 Poor Quality and Quantity of Manpower

Lack of trained and experienced manpower is a major hindrance to industrial security in Nigeria. Well-qualified security personnel are generally in short supply taking the country as a whole-, but it is believed that though many establishments have such capable security

staff, their talents are hindered or diluted by a combination of other related forces, prominent of which is limited education, professional training and experience.

3.4.3 Dearth of Modern Equipment, Technology and Methods

In these days of rapidly evolving technology, instantaneous communication and dynamic methods, the Nigerian industrial security manager lacks the necessary equipment, technology and methods for the prevention of security incidents. Delays in technical innovations, ignorance of existing alternatives are all manifestations of inexperience and no-knowledgeable top management.

3.4.4 Negative Work Attitudes

The ghost of "White man's work": is still hunting many Nigerians. Often this is accentuated by ethnic patronage and tribalism, and the results are quite detrimental to the company. "White man's work" makes it possible for one to be indolent without immediate retribution, for discipline to be remote and circuitous, for tenure and promotion to be unaffected by efficiency and productivities.

Work attitudes cover not only personal operational efficiency but also general security ethics, such as attitude to members of the public, sense of personal responsibility over equipment, sense of attachment to the company itself and willingness to make sacrifices in order to promote its interests.

It also involves a phenomenon, which makes people to be more loyal and more attached to a group than to the company. This is where decisions and exercise of authority deliberately favors one person or group of persons at the expense of the others. **A** situation where the zeal and ability of a security manager or supervisor is thwarted when his subordinates are hostile and conspire against him, causing him either to Compromise or to be removed, if their conspiracy reaches top management.

The other manifestation is where a security manager has to connive at the misdeeds of his kith and kin. Both cases are capable of frustrating any level of ability, if the collusions are not uprooted quickly and completely.

3.4.5   Financial Constraints

The security department of most companies suffers inadequate budgetary allocation. Insufficient or lack of finance is one of the major

problems facing security departments of most companies. Everything depends on finance. Whatever you do must, at the end of the day, translate into monetary terms. Nothing works without adequate financing.

3.4.6 Bribery and Corruption

Otherwise known as the "Nigerian factor" is a clog in the wheel of the prevention of security incidents in Nigeria. As long as personnel who are prone to bribery and corruption operate the security system, it will be difficult to attain optimum results operationally. Man is an important factor in the prevention of security incidents. He initiates actions, manipulates the tools and makes decisions.

3.4.7 Lack of Coordination

Improper coordination of activities spell doom on any security system. On a more routine level, efficient coordination should handle the company's security personnel in such a way that optimum services will be extracted from it. Balance in overall sectional work force, proper structuring of work schedule and loads. Prompt and effective system of discipline, regularity of wage payments, regularity of, and fairness in staff co-ordination's techniques still not attained in many companies. When these are put in place, attitudes to work and overall performance will be affected.

It has been argued that practical incentives in the form of bonus, special promotions, prizes, etc, should be freely applied to staff, so as to create the desire for excellence and. better service. But one could also argue that the same objective would be attained by judicious combination of effective discipline, better education and training for security personnel.

Lack of formation of data banks on crime and criminals' activities, other vital information about people and places, for instant reference, make the job difficult.

No meaningful effort has been made in Nigeria to integrate the public and private security systems. There exist no institutional arrangements for exchange of information between the two systems or for dealing with security problems- no common operational formula, etc. thus dualism still feature in the security set up. As a result of these, the security system is ineffective in the country.

SELF-ASSESSMENT EXERCISE 2

How useful are the roles of Industrial Security today?

3.4.8   Top Management Perception

Perception means the process by which individuals assess information from the environment, organise it and make out meaning from it. A company's point of view determines its security policies. If a company's point of view gives priority to fire prevention, then the security manager they appoint will be probably an ex-fireman who knows very little or nothing about crime and crime Prevention. If safety takes precedence over security boardroom discussion, they will appoint a full-time safety manager probably with engineering qualification who, must be trained as to site patrol, access control, fire precaution arrangements etc, and his main interest will center on safe working of plants. He will require deputies to take charge of crime and fire aspects of his job content. If the top management prefers crime prevention and control, they will appoint a full time industrial security manager who will also be asked to take responsibilities of fire prevention, safety welfare matter.

3.5   Types of Extent of Losses (Direct/Indirect)

For our purpose, means an action or 'Instance of failing to keep, maintain or use organisation asset. It involves taking away from an organisation or person, to deprive, to dispossess, to waste, to ruin or to destroy assets. It could be man-made or environmentally caused.

Losses fall into two broad classes' direct loss and indirect loss. These require definition.

Direct losses are losses that can be directly identified with specific security incident, as in the case of Jesse oil spill of October 1998, in which the PPMC/NNPC incurred a loss of thousands of naira that resulted from pipeline failure. These include the cost of about 30,000 barrels of crude oil spilled into ecosystem, the cost of replacing the damaged pipeline and the cost of environmental clean-up.

Indirect losses, on the other hand, are losses that cannot be directly identified with specific security incident. They are induced by direct losses and are not easily quantifiable. They are impacts of the direct loss on the nation and its peoples. E.g. the Jesses oil spill of October, 1998 induced fires, destroyed over 1,000 human lives, arable lands, viable economic crops, swamps and creeks with their teeming sea lives, vegetation, fishing ponds, homes and the general degradation of natural habits, human infertility, health and other social problems and so on. These losses (direct and indirect) are devastating when considered in terms of cost in time, cost in money and cost in all other resources.

3.6   Causes of Loss

Generally losses are caused or occasioned by various factors. These include-

3.7   Institutional or Organisational Factors

These could be explained as follows.

1.   Inadequate security control, whereby the system of security instituted is not effective, or the security department is not well established with qualified personnel and clear terms of reference, and authority, and responsibility. The security may also be improperly designed, and any improvement suggested may not have been implemented. There could also be poor management.

2.   Lack of organisational rotation of security operatives, especially those in sensitive areas like store, cash office, gate etc.

3.   Non-involvement of external security consultants. Security is so complex a subject that it may be wise to seek external expert advice occasionally.

4.   Heavy volume of work for security operatives (where there are few security operatives manning beats).

5.   Large span of control and hence making co-ordination difficult.

6.   Lack of proper security over premises, offices, materials documents, information, cash and even staff.

7.   Inexperience among security operatives and lack of control.

8.   Poor hygiene-motivation factor arrangements 'due to inadequate organisational infrastructure, security equipment and so on.

9.   Redundancy, allowed among employees and hence the creation of frustration.

3.8   Environmental/Social Factors

These are as follows.

1.   Lack of corporate culture against crime whereby unnecessary competition for the acquisition of wealth exists. Morality is ignored. There is unquestioning attitude of people toward sources

of wealth of other people, and there is the habit of not reporting theft, fraud, pilferage, murder and other criminal cases even when its committal is evident.

2. Socio-economic conditions like the extended family system which leads to primordial pursuits, poverty and unemployment.
3. Slow prosecution of cases including theft, fraud, pilfer, murder and other criminal cases.
4. Lack of heavy punishment meted out to offenders (with only dismissal as the usual punishment for extreme cases).

3.9 Individual Factors

These consist of the following.

1. Refusal to set good example in virtuous living, whereby honesty is protected as the best policy.
2. Lack of assessment of situations based on individual precepts rather than bad wagon tendencies.

4.0 CONCLUSION

Improved environment, better education, professional training and development contributes socially to the growth of security business ,while improved infrastructure like modern communication and crime combating facilities, electronic security devices coupled with purposeful motivation could help the security department to perform better, thereby enhancing the profitability of the company.

5.0 SUMMARY

We have explained the importance of business security and the company business with all the rights through its organs or Agencies for gains and profits.

We further discussed the opportunities of public and private security Agencies, their roles, environmental and social factors, problems of the security industry, including the extent of direct and indirect losses in the security industry. The basic facts of security business and the practice measures have also been explained.

6.0 TUTOR-MARKED ASSIGNMENT

1. Mention two career opportunities in the security industry.
2. Explain three problems militating against industrial security in Nigeria.
3. What do you understand by the term "Losses fall into broad classes"?

7.0   REFERENCES/FURTHER READING

Alla, O. (1997). *Security and Safety: Setting up Industrial Security Business*. Lagos: Spectrum Books Ltd.

Ekhomu, O. (2004)." The Role Industrial Security Provides in Era of Work Place Violence and Security, Shell Club Port Harcourt." *Shell Club Security Journals*.

Vroom, H.V. (1984). *Work and Motivation*. New York: John Wiley and Sons.

UNIT 4   PRIVATE SECURITY OPERATION IN THE PAST

CONTENTS

1.0   INTRODUCTION

'There are two great preoccupations in the lives of people and organisations. The first is that people make great efforts to acquire wealth and live for an eternity. The second is their great efforts to secure them. With such drives, we have notice for efforts around town for security of lives and property.

2.0   OBJECTIVES

At the end of this unit, you should be able to:

- identify two great preoccupations in the lives of people and organisation
- state the regulations of security industry
- state the private protection of lives and property
- state government protection of lives and property.

3.0   MAIN CONTENT

3.1   Private Protection of Lives and Property

Private arrangements are made such as burglar alarms, barricaded doors and windows, and even the acquisition of firearms. Other joint efforts are made as people arrange for neighborhood watches, e.g., vigilantes. There has been a clamour for state police force. Of recent Nigeria has witnessed an emergence of militant groups such as the Bakassi Boys, the Odua People's Congress etc in order to douse the rising scale of crime and spate of violence across the country? These increased concern and public participation are largely due to the general awareness, resulting

from the impact produced by the security sector on the national economy and the people.

3.2   Government Protection of Lives and Property

Government, also seeing the security of lives and property of its citizens as its responsibility had instituted agencies for protection and security: the chief reason for the existence of the Armed Forces, The Nigeria Police and so on.

SELF-ASSESSMENT EXERCISE

People make great efforts to acquire wealth and live for an eternity make great efforts to secure them. Do you agree?

4.0   CONCLUSION

Security in the lives and property of people include private security and government security. Other joint efforts are made as people arrange for neighborhood watchers such as vigilantes. These increased concern and public participation are largely due to the general awareness, resulting from the impact produced on the security sector, the National economy and the people.

5.0   SUMMARY

In this unit, you should have been able to analyse that security development entails opportunity for securing people's lives and property in Nigeria.

Also, we have noticed efforts of security Agencies in preventing the rising scale of crime and violence across the country. It is obvious that both spiritually and physically, security cannot be eradicated because it is part and parcel of human life.

6.0   TUTOR-MARKED ASSIGNMENT

1.   State why private security is more productive than the Government security.
2.   Mention two great preoccupations in the lives of people and organisation.

7.0   REFERENCES/FURTHER READING

Acha, K. (2003). *Security Manual.* Port Harcourt: Sakeche, Publishers

UNIT 5 DIFFERENCE BETWEEN PUBLIC AND PRIVATE SECURITY AND THEIR RELATIONSHIP

CONTENTS

1.0   INTRODUCTION

Generally, the National Security Council is the body charged with the responsibility of advising the president on matters relating to public security, including matters relating to any organisation or agency established by law, for ensuring the security of the nation and its people.

2.0   OBJECTIVES

At the end of this unit, you should be able to:

•   state what Public Sector Security is
•   define the Nigerian Police
•   state the duties of the Nigerian Police
•   differentiate between Private Security and Macrosecurity.

3.0   MAIN CONTENT

3.1   Loss Prevention and Activities

Under Private Security, most firms are privately owned and managed, while the public security refers to security (loss prevention activities) that is undertaken by state or agencies of the state. The Pahek Security Service, DOUGLAS Veteran Security Limited, PAVILION Security Holding Limited, etc. all come under the term Private Security, while agencies like the Armed Forces, the Nigeria Police, the Fire Service, Immigration, Customs, Nigeria Security and Civil Defense Corps, etc. come under the term 'Public Security' or 'Public Sector Security'.

3.1.1 The Judges Rules and Laws

Under Private Security, everybody is free to engage in whatever security activity he pleases, but subject to the Private Guards Companies Decree 33, of 1986 and other laws imposed by the state in the public interest-, he is perfectly free to follow his inclinations and to use his judgment and initiative at his own risk. He can decide for himself what part he will play on the security stage.

3.1.2 Characteristics of Private/Public Security

Private Security is characterised by competition. Firms compete with one another in sale of similar security products or service. The public security is invariable a monopoly.

3.1.3 Comparisons of Public and Private System in Loss Prevention

The Nigeria Police is a public institution established by the Nigeria police Act CAP 154 of 1943, for general crime prevention and law enforcement, while the Private Security firms are private companies required by law to be registered with the corporate Affairs Commission, and obtain an approval, License from the Ministry of Internal Affairs.

3.1.4 Duties (Public/Private)

The Nigeria Police is "employed for the Prevention and detection of crime, the apprehension of offenders, the preservation of law and order, the protection of property and the due enforcement of all laws and regulations with which they are directly charged, and shall perform such military duties within and without Nigeria, as may be required of them by, or under the authority of this or any other Act"_ (The Nigeria Police Act CAP 154 part 11 Section 4). The Private Security Services are

employed to "Perform the services of Watching, Guarding, Patrolling or Carrying of money for the purpose of providing protection against crime".

SELF-ASSESSMENT EXERCISE

Differentiate between the authority of the law that empowered the public and private security firms to operate.

3.1.5 Legal Powers of Operations

The Nigeria Police has <u>special</u> powers and are backed by the full force of law within which they operate. The Private Security normally has no special <u>legal powers</u>. He is a civilian, a citizen and enjoys the same rights and observes the same obligations under the law of sections 12, 13, 14, of Criminal Procedure Act as a citizen, in respect of arrest and disposal of offenders, detention, prosecution, indictment, investigation etc.

3.2   Constitutional/'Responsibilities

The Nigeria Police is a body answerably to the President through the Inspector-General of Police. The Nigeria Police Council and Police Service <u>Commission are constitutional</u> bodies responsible for the organisation, administration and general supervision of the Nigeria police force and all matters relating thereto. (See Section on Regulation of Security Industry for details). The private security is ruled by several management policies on security. The company policy forms the source from which all security actions evolve. More so, the private security presently lack control, monitoring and supervision in Nigeria. As such, the Immigration has attempted to monitor them to ensure that no foreign expert is involvement in the business of security, and where there is partnership, to see that the person's involvement is not detrimental to the security of the country. The Nigerian Security and civil defense corps have also attempted to monitor and supervise the private security guards companies all to no avail because they lack the required legal powers. The Nigeria Professional Security Association is in the process of gaining the necessary legal powers to regulate, monitor, supervise and discipline private security.

3.2   Loss Prevention/Profit

The dominant motive of the private security company is profit. The Private Security Company is driven by economic <u>gains and</u> profit maximization, and this makes his decisions turn mostly on considerations of <u>loss</u> <u>or gain</u>. A profitable business thrives and grows.

A losing business sickens and dies. So profits become the driving forces that moves and guides him. On the other hand, a distinguishing feature of the public security is that unlike the private security, the profit motive is not stressed or dominant. Services are provided free of charge or are heavily subsidised. Service and welfare remain the driving forces that move and guides them.

3.3 Access of Information

The Nigerian Police, with its nationwide network and spread, have access to information than do the private security. However, the widespread opinion now is that the private security in the employ of companies has unbelievable minded persons. The reason for this is not difficult to discern. The private security officers are civilians, the live with the civilian population and interact well with them. The criminals and the criminally minded do not see them as dangerous coupled with the fact that they do usually links with the Police.

The Nigerian Police do not reckon with them and so people easily divulge information before them. The neighbourhoods also see them as harmless.

3.5 Training and Experience

The Nigerian Police has well-trained, well-motivated and physically fit personnel compared to some private security outfits in Nigeria, that are nothing more than collections of the unemployed, who do not know anything about **ABC** of security, not to talk of private security. They are weak in standards; the personnel lack training, are not well-motivated and are physically unfit by all standards.

4.0 CONCLUSION

In this unit, we have learned that without legal powers and special powers from the Authority of the Law, both public and private security organisations will not perform. The constitutional bodies like the Nigeria Professional Security Association (N.P.S.A) are also responsible for the security operations in the process of gaining the necessary legal powers to regulate, monitor, supervise and discipline private security.

5.0 SUMMARY

From the classical to human relations, protection, crime prevention and detection approaches to this study, are the limitations, characteristics and comparisons of proactive measures system in the profit motive, which is

not stressed or dominant on the private security. Public security is stressful and non profitable.

6.0   TUTOR-MARKED ASSIGNMENT

1.   In this modern society, private security has variables while the public security is   invariable a monopoly "Do you agree or not"?
2.   Does the law sections 12, 13, 14 of Criminal Procedure Act (CPA) provide a legal power or a right as a Citizen, to empower the private security to arrest any offender and prosecute after proper investigation?
3.   What roles does Nigeria Professional Security Association play in the Private Security Organisation.

7.0   REFERENCES/FURTHER READING

Charles, P.N. (1991). *Private Security and the Investment Process* (2nd Ed). New York: Butterworth Heinemann Books Ltd.

Girigiri, B. (2001).   *Industrial Relations in Nigeria*. Port Harcourt: Belppl Publishers.

MODULE 2

UNIT 1   DESIGN OF SECURITY SURVEY SYSTEM

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Content
      3.1   Definition of Security Survey
           3.1.1   Top Management Involvement
           3.1.2   Conducting Security Survey
           3.1.3   Evaluation of Loss Prevention Programme
           3.1.4   Determining and Maintaining Standard
      3.2   Survey Report
      3.3   Periodic Security Survey
      3.4   Maintaining Security Files
      3.5   The Use of Security Files
4.0   Conclusion
5.0   Summary
6.0   Tutor-Marked Assignment
7.0   References/Further Reading

1.0   INTRODUCTION

The goal of risk management cannot be achieved without reducing through a total management commitment, the number of incident that lead to losses. Before any risk can be eliminated or reduced, it must be identified. Security survey is the most valuable management tool in the process of risk analysis, which proceeds from threat assessment (identifying risk) to threat evaluation (determining the criticality and cost of that risk), to the selection of security countermeasures designed to contain or prevent that risk.

2.0   OBJECTIVES

At the end of this unit, you should be able to:

- determine the existing state of security survey
- locate weakness in its defense
- determine the degree of protection required
- recommend/establish a total security programme.

3.0   MAIN CONTENT

3.1   Definition of Security Survey

Security survey can be defined as a critical, on-site examination and analysis of an industrial plant, business, home, public or private institution to ascertain the present security status, to identify deficiencies or excesses, to determine the protection needed, and to make recommendations to improve the overall security.

3.1.1 Top Management Involvement

In order to ensure that adequate funds for the undertaking are available and to guarantee the cooperation of all personnel in the facility, the motivation setting the security survey in motion should come from top management.   Since a thorough security survey will require an examination of procedures and routines in regular operation, as well as an inspection of the physical plant and its environs, management's interest in the project is of the highest priority.

3.1.2 Conducting Security Survey

The security survey may be conducted by staff security personnel or by qualified security specialists employed for this purpose. Some experts suggest that outside security people could approach the job with more objectivity and would have less of a tendency to take certain areas or practices for granted, thus providing more complete appraisal of existing conditions.

Irrespectively of who conducts the survey, it is important that they have training in the field and that they have achieved a high level of ability. It is also important that at least some members of the security survey team be totally familiar with the facility and its operation.

Without such familiarity it would be difficult to formulate the security survey plan. The security survey itself must be planned in advance in

order to make the best use of personnel and study the operation in every phase.

SELF-ASSESSMENT EXERCISE

What steps can you take before any risk could be eliminated or reduced?

3.1.3 Evaluation of Loss Prevention Programme

Security Survey planning involves developing an overall strategy for the expected conduct and scope of the examination. The nature, extent, and timing of planning vary with the size, complexity and knowledge of the business or facility. In planning the examination, previous studies and recommendations should be considered. These should be studied for any information they may offer.

Secondly, include a check-list or security survey programme made up by the survey team, in preparation for actual inspection. This list or programme will serve as a guide and a reminder of areas that must be examined and, once drawn, should be followed systematically. In the event that some area or procedure has been omitted in the preparation of the original checklist, it should be included in the inspection, and its disposition noted in the evaluation and recommendation.

Security Survey planning requires a preparation of a survey programme or check list, which is asset of written instructions to be followed by the security personnel, or by qualified security specialists during the study. The security survey programme or check-list should be spelt out in detail, and should show the procedures that are necessary to accomplish the study objectives.

3.1.4 Determining and Maintaining Standard

Since no two companies are alike (not even those in the same business), no check-list exists that could universally apply for every survey purposes.

3.2 Survey Report

The survey must document the full scope of its examination. Thereafter a report should be prepared indicating those areas which are weak in security, and recommending those measures which might reasonably make the security of the organisation Lip to acceptable standard. On the basis of the status as described in the survey, and considering the recommendations made, the security plan and procedures can now be drawn up to do the following.

- Protect against internal and external theft, etc.
- Develop access control procedures designed to protect the facility perimeter, as well as computer facilities located internally.
- Establish lock and key control procedures.
- Design, supervise, and review installations of anti-intrusion detection
- Systems.
- Establish an executive protection programme for corporate personnel here and abroad, to deal with extortion and kidnap problems.
- Provide control over the movement and identification of employees, customers and visitors on company property.
- Review the selection, training and development of security personnel, proprietary or contract.
- Assist in the establishment of emergency and disaster plans and guidelines.
- Identify the internal resources available and needed for the establishment of an effective security programme
- Develop and present instructional seminars for management in all of the above areas.

Certain circumstances warrant compromises. The sitting of the company or the area involved, for instance, may make the ideal security programme of full coverage of all contingencies, too costly to be practical. In such cases the plan must be re-examined, to find the best approach to achieve acceptable security standards within those limitations. Let it be understood that the security manager will rarely get all of what he wants to do the job. As in every department, he must find hardware within the framework of the possible result. Where he is denied extra personnel, he must find hardware that will help to replace them. Where his request for more coverage by CCTV is turned down, he must develop inspection procedures or barriers that may serve a similar purpose. If at any point, he feels that he has been cut to a point where the stated objective cannot be achieved, he is obliged to communicate that opinion to management, who will then determine whether to diminish their original objective or authorise more money. It is important that security manager exhaust every alternative method of coverage, before he goes to management with an opinion that requires this kind of decision.

3.3 Periodic Security Survey

After the security plan has been formulated, it is essential that the survey process be continued. For a security plan to be effective, it must be dynamic. It must change regularly in various details to accommodate

changing circumstances in a given company. Only regular inspections can provide a feel for the needs of the operation, and only periodic surveys can provide a basis for the ongoing evaluation of the security status of the company. Exposures and vulnerability change constantly; what may appear to be minor alteration in operational routines may have a profound effect on the security of the entire organisation.

3.5   Maintaining Security Files

The survey and its resultant report are valuable in the building of security files. This evaluation reveals a detailed current profile of the company's regular activities. Such a file enables the security department to operate with increased effectiveness, but it should, by inspections and regular surveys be kept current.

The data base could be augmented by texts, periodicals, official papers and relevant articles in the general press related to security matters. Special attention should also be paid to subjects of local significance. Although national crime statistics are significant and help to build familiarity with a complex Subject, local conditions have a more immediate import to the security of the company.

3.6   The use of Security Files

As these security files are enlarged they will become increasingly useful to the security operation. Patterns may emerge, seasons may become significant, economic conditions may predict events to be alert to.

(a)   Certain days or seasons may emerge as those on which problems occur.
(b)   Targets for crime may become evident as more data is amassed. This may enable the security manager to reassign priorities.
(c)   A profile of the type and incidence of crimes (if possible, even the criminal himself) may emerge.
(d)   Patterns of crime and its <u>modus operandi</u> on payday or holiday or weekends may become evident.
(e)   Criminal assaults on company property may take a definable or predictable shape or description, again enabling the security manager to better shape his countermeasures.

The careful collection and use of data concerning crime in a given company could be an invaluable tool for the conscientious security manager. It can add an important dimension to his regular re - examination of the status of crime in his company

4.0   CONCLUSION

Security Survey planning involves a lot of commitment, timing of planning vary with size, knowledge complexity. Another process requires a preparation of survey programme, which is asset of written instructions to be followed by the security personnel. However, without familiarity with the operation and its facility, it would be difficult to formulate the security survey plan, and the survey system itself must be planned in advance for the successful operation.

5.0   SUMMARY

In this unit, we studied security survey which is the most valuable management tool in the process of risk analysis, evaluation of loss prevention programme, determining and maintaining standard. The problems of security survey check-list should be considered in making recommendations and evaluation to improve the overall security.

6.0   TUTOR-MARKED ASSIGNMENT

1.   Define security survey system.
2.   Why is it necessary to conduct security survey?
3.   What are the necessary procedures to accomplish the study objectives of Evaluation of loss prevention programme?

7.0   REFERENCES/FURTHER READING

Okiro, M.M. (2004). *An Address Delivered during Tackling the Challenges of Law Enforcement in Nigeria*. Port Harcourt: Shell Club.

Braimoh, A. (2001). *The Basics of Security Knowledge*. U.S.A.: New World Press.

UNIT 2   THE STATE OR NATIONAL INTEREST

CONTENTS

1.0   INTRODUCTION

This Unit, Module 2, will focus on the overview of Principles and issues in Security Management. It will also further examine the challenges embodied in various aspects of security such as Personnel, facility and information; principles of crime prevention and control, and the protection of assets respectively. You are also employed to use the situational analysis, case studies and other research-oriented approaches.

2.0   OBJECTIVES

At the end of this unit, you should be able:

- state the principles and control of the regulations in the security Management
- state the composition of the National Security Council
- specify how the Nigeria Police Council functions with the responsibilities of Police Service Commission
- explain the legitimacy and requirements of private Security and how to own Security Guard Company.

3.0   MAIN CONTENT

3.1   National Security Council Responsibilities

The National Security Council is a constitutional body responsible for advising the president on matters relating to public security, including matters relating to any organisation or agency, established by law for ensuring the security of the nation (life and property).

3.1.1 Composition of the Executive Members

The National Council comprises the following members:-

- the President who is the chairman
- the vice-President who is the Deputy-Chairman
- the Chief of Defense Staff
- the Minister of internal-Affairs
- the Minister of Foreign-Affairs
- the National Security Adviser
- the Inspector-General of Police. and
- such other persons as the President may in   his discretion appoint.

3.1.2 Nigeria Police Council

The Nigeria Police Council comprises the following members:-

- the President who is the Chairman
- the Government of each state Of the Federation
- the Chairman of the Police Service Commission, and
- the Inspector-General of Police

3.1.3 The Functions of the Nigeria Police Council Include

a)   The organisation and administration of the Nigeria Police Force and all other matters relating thereto (not being matters relating to the use and operational control of the force or the appointment, disciplinary control and dismissal of members of the force).
b)   The general supervision of the Nigeria Police Force, and
c)   Advising the President on the appointment of the Inspector-General of Police.

3.1.4 Police Service Commission

The Police service Commission comprises the following members:

a.   A Chairman and
b.   Such number of other persons not less than seven but not more than nine, as may be prescribed by the act of the National Assembly.

The Commission is responsible for

a.   Appointment of persons to office (other than the office of the Inspector-General of police) in the Nigeria Police Force, and
b.   Dismissal and exercise of disciplinary control over persons holding any office referred to above.

c.   According to the Nigeria Police Act CAP 359 Laws of Nigeria Section 10 (i). the president may give to the Inspector-General such directions with respect to the maintaining and security of public safety and public order (security), as it may consider necessary, and the Inspector-General shall company with those directions or cause them to be complied with.

3.1.5 The Private Security-Organizations

In their book, "Introduction to Ssecurity Management and Planning" Fisher and Green (1986) noted, "Citizens fear of crime and awareness that criminal justice resources alone cannot effectively control crime, has led to a growing use of individual and corporate protective measure, including private security products and services, and neighborhood based crime prevention. Law enforcement resources have stabilised and in some cases declined.

This mandates greater cooperation with the private security resources to jointly forge a partnership on an equal basis for crime prevention and reduction. Law enforcement can still afford to continue isolating, and in some cases ignoring this important resources and technology, may be the one viable option left to control crime in our communities. These views of Messrs Fisher and green were well noted that security in its entirety can hardly be provided by public organisations alone. The Government is aware of this and decided to enact the **private Guards Companies' Decree No. 33 of 1986** for the purpose of providing for, and regulating the conducts of private guards operators.

SELF-ASSESSMENT EXERCISE 1

State the composition of Nigeria Police Council.

3.2   Duties of Private Security Company

Security guard companies are empowered to perform the service of watching, Guarding, Patrolling or Carrying of money for the purpose of providing protection against crime.

3.2.1   Requirement of Private Security Guards Company

The requirements/procedure for setting up private security companies is as follows:

a.   Register the company with the corporate-Affairs commission.
b.   Apply to the Minister of Internal Affairs for duplicate copy of the license to be given to you, in case the original gets lost or is defaced.
c.   Company to be wholly owned by Nigerians
d.   Application for license must contain form A.
e.   If dogs or other animals are to be employed, all existing regulations related to animal health and certification must be complied with.
f.   The license, which shall specify the number of offices, branch or other places of business which the company is permitted to maintain, shall be valid for two years.
g.   On the day of registration the company shall notify the licensing authority with the addresses (not P.O. Box) of all its branches in Nigeria. Any change in address must be communicated to the licensing authority within 14 days of such change. None compliance with (1) will make the company and every liable to a fine of N500.00.
h.   License must be displayed in a conspicuous place in the office (company office). Photocopies could be used in the branches.
i.   All employees must be approved by the minister of internal affairs. Application for approval forms C. Approval form D. Identity Card to be issued to the employee by the security company. The employee should carry the 'I.D. Card when on duty and produce it for inspection when asked by a Police Officer or other whom he may be dealing with. It is subject to renewal.
j.   The Minister must first approve the training syllabus and instruction note meant for employee of the company.
k.   Uniform, Cap, Badge, accoutrement -or other identification marks (to be used) have to be approved for usage by the Minister.

3.2.2 Ineligibility to Own Security Guard Company in Nigeria

Any person may be ineligible to own security guards Company in Nigeria if:

a.   Convicted of criminal offence in Penal code, Criminal code, Firearms Act, Explosive Act or Robbery/Fire arms Decree.

b.   Convicted of offence involving fraud, theft or breach of trust in Nigeria or elsewhere.

C.   Dismissed, discharged or removed on disciplinary grounds from the Police, Arm Forces of the Federation, Prison Service, Special constabulary, Fire service, customs or any similar law enforcement agency in Nigeria or elsewhere.

d.   Who is not a citizen of Nigeria?

3.2.3 Prohibited Activities/Offences

A private security guards company/staff

a.   Should not act as a debt collector or advertise it as carrying out such services.
b.   Should not act as a member of the police force or perform the duties of a police officer or any other law enforcement agent.
c.   Should not refer to itself, as -Private Detective" or hold himself out in any manner as a private detective.
d.   Should not illegally divulge information received in the course of his duty.
e.   Any person who does as follows.

i.   Gives false information during application for license,
ii.   Act as an employee of company without license,
iii.   Fail to carry I. D. Card or produce it on demand,
iv.   Wears, carries, or bears any of the articles mentioned above which he is not authorised to carry or wear"
v.   Bears or possesses any bureau or ammunition.
vi.   Supplies or offer to supply any bureau, ammunition, tear gas or similar manufactured weapons-, or
vii.   Collects, or offers or attempts to collect or directly or indirectly engage in the business of collecting debts or claims of any land, are guilty of an offence:

- Advertisement on Radio, TV, Newspaper about his services other than advertisement for recruitment of staff without specifying the name and address of the company.
- Company or staff who sells, disposes of or delivers, lets out, hires or rent its license, approval or I. D. Card to another person or permit any person to use the license, approval or I.D. Card.
- Unlawfully entering any premises.
- Falsely or otherwise makes any person to enter into a contract with him.
- Employment of person, refused approval by the Ministry.

3.2.4 Punishment under the Private Guards Security Companies Decree

Apart from the offences relating to firearm, for which the person shall be punished as prescribed under the Firearms Act or any other relevant enactment, individuals will be liable to a fine of N400.00 or 12 months imprisonment or both, while company (corporate or not) are liable to a fine of not less than **N** 500.00.

1   The following persons are included:

a.   Every Director, Manager, Secretary or other similar officer of the corporate body.
b.   Every partner or officer of the firm.
c.   Every person concerned in the management of the affairs of the association.
d.   Every person purporting to act in any such capacity as afore-said, in any corporate body, firm or association, shall severally be guilty of that offence, and liable to be prosecuted and punished as if he had himself committed the offence in an individual capacity-, unless he proves that the act took place without his knowledge, consent or connivance.

2i.   Company or staff who sells, disposes of or delivers, let out, hires or rent its license, approval or I.D Card to another or permit any person to use his license approval or I.D Card.
ii.   Unlawful entering any premises.
iii.   Falsely or otherwise make any person to enter into a contract with him.
iv.   Employment of person refused approval by the Ministry.
v.   The license of the company can also be revoked where the company   contravenes any provisions of the Decree.

3.3 Deployments and Control of Supernumerary Police Officer

This refers to a police officer appointed following an application by any person (including Public or Private Organisation) who desires to avail himself of the services of one or more police officer, for the protection of property owned or controlled by him. Examples of supernumerary police include shell police, Elf police, Agip police, Nafcon police, etc.

3.4 Process of Appointment of Supernumerary Police Officer

a. A formal application to the Inspector of Police stating the nature and situation of the property in question, and giving such other particulars as the inspector General of Police may require.

b. The Inspector General with the approval of the President directs the appropriate authority to appoint as supernumerary police officer in the force, such number of persons the Inspector general of thinks as requisite for the protection of the property to which the application relates, if satisfied.

c. The President authorises the appropriate authority to appoint persons as supernumerary police officers in the force under and in accordance with authorisation.

d. Every authorisation shall be in writing and shall specify the police area to which it relates, and the maximum number of supernumerary police officers who may be appointed under that authorisation.

e. Every supernumerary police officer appointed under an authorisation, shall be appointed in respect of the area of the police division command in which the property he is to protect is situated.

f. Shall be employed exclusively on duties connected with the protection of   that   property, or the administration or maintenance of those premises

g. Shall in the police area in respect of which he is appointed, but not elsewhere, have powers and privileges and immunities of a police officer.

h. Subject to the restriction imposed by paragraph (iii) above and not   provisions of section 22 of the Nigeria Police.

SELF-ASSESSMENT EXERCISE 3

Mention the reasons why you cannot own private security company.

i.   Act CAP 359, shall be member of the force for all purpose and shall accordingly be subject to the provisions of this Act ,and in particular to the provisions to discipline.
ii.   Where any supernumerary police officer is appointed, it is the responsibility of the person (or organisation) availing himself of the services of that officer to pay.
iii.   The full cost of the officer's uniform.
iv.   The officer's salaries and such additional amounts as the Inspector General may direct to be paid in respect of the maintenance of the officer.

4.0   CONCLUSION

The Nigeria Police Force as the constitutional body set up by the State to provide internal security in crime prevention, has been discharging its responsibility with increasing challenges. Several factors have been put forward for the steady rise in criminal activities.

Recently, the general economic depression has worsened the situation. Nigerians fear of crime and awareness that criminal justice resources alone cannot effectively control crime has led to a growing use of individual and corporate protective measure, including private security products and services, and neighborhood based crime prevention. It is not gainsaying that Nigeria law enforcement resource have stabilised and in some cases declined. This mandates greater co-operation with the private security resources to jointly forge a partnership on an equal basis for crime prevention and reduction. Nigeria law enforcement can ill afford to continue isolating and, in some cases, ignoring this important resources.

5.0

The creative use of private security human resources and technology is one viable option left to control crime in Nigeria. Public establishment alone can hardly provide the security of society in its entirety. The Federal Government of Nigeria is aware of this and decided to enact the -Private Guards Companies Acts" of December 15, 1986 for the purpose of providing for and regulating the conduct of private security practitioners. This chapter discussed all the essential aspects of the private security Guard Companies Decree No. 33 of 1986 and institutions charged with the responsibility of regulating organisations responsible for protection of lives and property.

6.0   TUTOR-MARKED ASSIGNMENT

1.   State the composition of National Security Council.
2.   Why should private security companies partake in the escorting of money and preventing of crime?
3.   What is the meaning of the following:-

a.   NSC
b.   NPF
c.   SPY

7.0   REFERENCES/FURTHER READING

Momodu, B. (2001). *The Basic of Security Knowledge and Planning*. Lagos: Olucity Press Ltd.

Hill, G.W.L. & Pickering, J.P (1986). "Divisionalisation, Decentralisation and Performance of Large United Kingdom Companies:" *Journal of Management Studies* (JMS), Nigeria Police Regulations, Law books and Police Acts Manuals.

UNIT 3   OPERATIONAL DUTY FOR SECURITY STAFF, SUPERVISORS AND MANAGEMENT FUCNTIONS

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Content
         3.1   Proforma Schedule of Duty for Security staff
         3.2   Proforma Schedule of Duty for Supervisory Staff
         3.3   Structural Organisation Chart of Industrial Security Management Department
         3.4   Academic Research for Security Knowledge
         3.5   Knowledge of Security
         3.6   Training and Functions of the Security Manager
         3.7   Qualities of Industrial Security Manager
4.0   Conclusion
5.0   Summary
6.0   Tutor-Marked Assignment
7.0   References/Further Reading

1.0   INTRODUCTION

It is customary for every industrial or commercial firm to write out schedule of duty for security staff in the enterprise. This is to enable both the employer and employee acquaint themselves properly with the nature of the job at stake, and the demanding conditions surrounding it. Such arrangement should be necessary in every security department.

2.0   OBJECTIVES

At the end of this unit, you should be able to:

•   specify the demanding responsibility in an officer' s schedule of duty
•   defend why operational errors and mistakes committed by security staff should not be over flogged state the importance of schedule of duty
•   describe how to keep in constant touch with operational realities
•   explain managements policy towards schedule of duty and the general rules through which they are applied.

3.0   MAIN CONTENT

3.1   Proforma Schedule of Duty for Security Staff

The following schedule of duty is prepared for security operatives and they should be encouraged to constantly read and practicalise it.

It reads as follows.

1.   You are expected, as a matter of necessity, to receive, read, memorise, and practicalise your schedule of responsibility as long as you are in the service of security organisation.
2.   You are to ensure the protection of properties of the company at all times against theft or malicious damages, be it committed by employees or an intruder.
3.   You are to ensure that all the regulation s of the company affecting the security of its property is properly carried out without ambiguity, contempt or sentiments.
4.   You are to ensure the protection of the company's inventories, information, cash, equipments, materials, building and its contents against damage by fire, flood, bad weather condition, or insects.
5.   You are to pay attention at all times to electrical installation water systems, steam turbines, gas cylinders, fuel tanks, and pipes to detect breakdown of the systems, leakages, wastage, sparks, overheating at all times, and take immediate action necessary in the interest of safety and security, to stop or salvage it.
6.   You are to ensure that all fire- fighting equipment are serviced, refilled and fully operational and remain in the designated areas, for immediate accessibility in times of emergency.
7.   You are to ensure the prevention of unauthorised vehicles or persons from gaining access or entry into the premises especially when such entry will pose threat to the security of life and property.
8.   You are to ensure that no employee, visitor, contractor, ex-staff, vendor etc. leaves the premises in an irregular manner.
9.   You are to ensure that all visitors are courteously received assisted appropriately, directed in a manner which reflect the company's credited. And equally record the details of such visits as required by security protocols.
10.   You are to take part fully or partially in recording all company vehicles leaving or coming into the premises empty or loaded, to collect or deliver goods, and check such goods and demand the gate pass as mandate by security protocols
11.   You are to ensure that no tool, equipment, vehicle or inventory leaves the premises on weekends, Sundays and holiday periods,

without an official permit from the company of whose property you are protecting. No argument or threat should bend you to allow the passage of such properties in the absence of the official permits.

12.   You are to regulate the movements of trafficking within the premises of the company, and equally organise and control the appropriate parking of vehicles while in the company's premises.

13.   You are to respond to radio or telephone calls and ensure that important messages are recorded and passed to the intended recipient with speed and efficiency.

14.   You are to accept, act upon, or pass any message received from the company drivers, officers, clients, other companies, the Police, fire service, NITEL, NEPA, CUSTOMS and law enforcement agencies of vital security importance to the company especially emergency matters, during quiet weekend or holiday periods.

15.   you are to accept and check the weight-tickets handed down by the drivers of loaded vehicles leaving the company/stores/warehouses and ensure that the figures recorded thereon do not reveal weights in excess of the permitted load, and equally take the necessary action of notifying your officer/supervisor and the central dispatch depot or the company dispatch office when contravention is detached.

16.   You are to accept, record and pass with speed any call of precautionary nature from the police, company officers, and your colleagues in other locations, or any other source adjudged to be legal and reliable to your nearest security coordinator, security officer or supervisor for immediate action.

17.   You are to respond at anytime to the operation of alarm system or an intruder both in day and night, by putting into immediate effect the prearranged security plans and techniques to control such eventualities.

18.   You are to ensure all duties are performed in uniforms with your ID card permanently hanged on your chest or the front pocket of your shirt wherever you are in the company's premises.

19.   You are to ensure all equipments, working tools and uniforms are kept to take instructions from damage and abuse.

20.   You are to take instructions from your superiors and you can equally offer advice or suggestions of vital security importance when doing so. This will best serve the interest of the company.

21.   All instructions on security matters given to you by your superiors from time to time are confidential and shall not be discussed or communicated to anyone outside the department or company.

22.   You are strictly expected and directed to keep yourself informed of all instructions affecting your duty and of any amendment (s)

that may be made in respect of changing operational policies and procedures in the company, as may be directed or redirected by the management.

23. You are expected through practice, training, seminars and workshop, to make yourself more proficient in all matters of security operations.

24. You will be required from time to attend internal or external training or courses to improve your proficiency.

25. All additions and amendments in this schedule of duty will only be made in writing and by the management of this company.

26. The basic duty requirements contained in this schedule of duty shall be diligently conducted in a manner consistent with the requirements therein, unless in situations demanding special measures or techniques where you will be required to use your experience or discretion.

27. The conditions of employment shall apply to you and your colleagues within the same rank profile.

28. Discipline is the backbone of any security operations. You are strictly instructed to be disciplined and respect all the statues affecting your official responsibilities, and equally avoid irresponsible behaviour capable of discrediting your image or the image of the company.

29. You are strictly expected to keep yourself neat and fit at all times of your official appearance on duty.

30. You will, from time to time, be expected to take decision affecting life and property. You are therefore strictly advised to use tact and intelligence, and do not do anything capable of jeopardising security of life, property or good industrial relations.

31. You will respond promptly to any call by your superior officers to perform overtime, wherever situations demand.

32. You will learn and acquaint yourself with the inconveniences of working alone in the night, and not entertain the fears of personal danger, which you cannot avoid by either hiding or running away.

33. You will acclimatise yourself to wearing your symbolic uniform which will make you stand out and attract questions to which you will be expected to know the answers.

34. You will from time to time, come under the instances of extreme provocation, and you will in such circumstances, have to control your temper.

35. Always remember that in security practices, the first impression is very important. Therefore always dress smartly, neatly, move briskly and respond to questions intelligently and confidently.

36. Whenever you are in doubt of anything ask your superiors.

37. Do not conceive mutiny or conspiracy to cause disharmony to the company. Report secretly and discretely such plots whenever it

comes to your hearing. However, do not engage in rumour-mongering, gossiping or blackmail in order to be noticed or elevated.

3.2   Proforma Schedule of Duty for Supervisory Staff

This schedule of duty is meant to acquaint superiors with their responsibilities. Supervisors should then be encouraged to read and memorise them. They are as follows.

1.   You, as a supervisor, must uphold a high standard of competence, good conduct, cleanliness, respectable appearance and integrity in a manner which reflects the best credit of the company.
2.   You are to supervise and ensure that no guard neglects his duty by sleeping, fallout, absenteeism, late-coming, unreasonable delay or failures to carry out his tasks, conducting personal affairs during working hours, refusing to render assistance or cooperate in the conducts of security operations during working hours.
3.   You are to ensure that there will be no disorderly conduct, use of abusive language, quarrel, intimidation, harassment or any disruptive activities which directly or indirectly interfere with the normal and efficient security operations.
4.   You are to ensure that no member of the guard-force team under your supervision possess, sell or consume intoxicants, drugs, or any substance capable of intoxicating, while on duty on the beat location.
5.   You are to ensure all guard-force under your supervision maintain a high level of loyalty, honesty, dedication, patience, reliability, respect and discipline in their daily activities in the beat location.
6.   You are to supervise and inspect all access areas and , pontential penetrating points i.e. fence ,   gates, windows, perimeter walls and locks to detect vulnerabilities that can easily be used by intruders.
7.   You are to ensure stability by seeing that all Instructions are carefully studied, understood and considered before issuing them.
8.   You are to preserve balance by ensuring a proper economy of efforts and resources to all allocated tasks within the job parameter, without ambiguity or confusion.
9.   All reports should be clearly, concisely and conscientiously written with efficiency.
10.   You are to guard against and -discourage sycophancy, redundancy, gossiping, double deception, misdemeanor and laziness during security operations in the beat location.

11.   You are to ensure that daily working orders, post orders, general orders statement and standing orders are clearly defined and stipulated for everyone to understand.

12   You are to ensure that flexible working arrangements are clearly studied and disseminated, so that no tasks fall between two jobs at the same time or clash of personality is recorded.

13.   You can delegate power, responsibility or task at lower, medium or higher grade in absolute trust and confidence, so that you have sufficient time to tackle other problems. However, that shall not be a guarantee for you to dodge your responsibility or become a boss.

14.   You are to ensure that while delegating duties and responsibility, the individual's capability is used as a yard stick for delegating such task and responsibilities.

15.   You shall closely monitor the guard-force in your locations according to their degree of skills, degree of discipline, degree of concentration, ability to work on conditions surrounding the job, degree of neatness, ability to work with less or no supervision, pleasing personality to customers and visitors, degree of tolerance, degree of patience, degree of courage, and degree of mental and manual efforts.

16.   You shall as a supervisor, develop a community of interests between the   individual guard in the team and the company as a whole.

17.   You shall, as a supervisor, make the individual on the team to feel the success of
the team is his own success, and the failure of the team his own failure.

I8.   You shall equally ensure that the team in which you belong realises its potentialities as a whole, and each individual recognises the part to play within the team as an integral whole.

19.   You shall daily supervise all safety systems and equipment and ensure that the daily precautionary measures are taken.

20.   You shall properly induct, instruct, guide, assist and supervise new guard-force members in your locations, until they develop enough experience and good working knowledge to fit in the company's operational standard,

21.   You are to ensure that the duties and the security of the beat locations are duly handed over to the incoming team before leaving the premises.

22.   You are to ensure proper record-keeping of documents, information, correspondents and matters relating to the routine security operations in our beat location.

23.   During the visit of any of the company's executive, you shall ensure that extra security measures are taken in and around

vulnerable points of strategic security significance, until the departure of the executive.

24.   You shall maintain absolute degree of fairness, justice, high sense of logical reasoning while arbitrating between parties in beat locations.

25.   You shall be a leader, not a boss, and prepare to lead by example by showing charismatic abilities, greater dexterity, wise counsel and offering to do first what ought to be done by all

26.   You shall learn to speak confidently, gently, respectably and courteously to both   your superiors and subordinates and remember only animals bark and shout.

27.   All instructions on security matters given to you by your superiors from time to   time are confidential matters, and shall not be discussed or communicated to anyone outside the security department or the company.

28.   You are expected to keep yourself informed of all instructions affecting your duty and of any amendment(s) that may be made in respect of changing operational policies and procedures in the company, as may be directed or redirected by the management.

29.   You are expected, through practice, training, seminars and workshops to   make yourself more proficient in all matters of security operations.

30.   You will be required from time to time to attend internal or external training or courses to improve your proficiency.

31.   All additions and amendments in this schedule of duty will be made in writing by the management of this company.

32.   The basic duty requirement contained in this schedule of duty shall be diligently conducted in a manner consistent with the requirement therein, unless in situations demanding extra measures or techniques where you will be required to use your experience or professional expertise.

33.   The conditions of employment apply to you and your colleagues within the same rank profile.

SELF-ASSESSMENT EXERCISE 1

Ineffective supervisory control can breach the security operations. "Is it true"?

3.3   Structural Organisation Chart of Industrial Security Management Department

Generally, there is no uniform structure of industrial security management department as it differs from business to business, chain to command and relationship to other office executives. But in practice the following illustration can be deduced.

ORGANISATION CHART OF INDUSTRIAL SECURITY DEPARTMENT

```
                    ┌─────────────┐
                    │  Board of   │
                    │  Directors  │
                    └──────┬──────┘
                           │
                    ┌──────┴──────┐
                    │   General   │
                    │   Manager   │
                    └──────┬──────┘
                           │
                   ┌───────┴───────┐
                   │ Chief Security│
                   │    Officer    │
                   └───┬───────┬───┘
              ┌────────┘       └────────┐
       ┌──────┴──────┐          ┌───────┴──────┐
       │   Safety    │          │   Security   │
       │   Officer   │          │   Officer    │
       └──┬───┬───┬──┘          └──────────────┘
         ( ) ( ) ( )          ( )  ( )  ( )
```
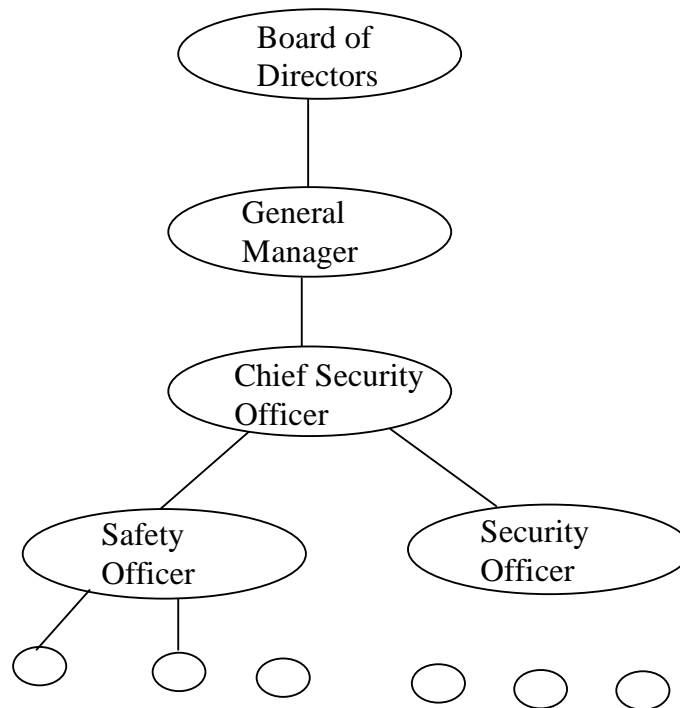
Representative Subordinated/Supervisors/Operatives

3.4   Academic Research for Security Knowledge

This involves technical theory, knowledge of the law, company rules and regulations, theoretical routine to be followed in any givien circumstance, alternative lines of action open, knowledge of equipment, its use, advantages and disadvantages and systems which are 'table in one circumstance but useless in another.'

3.5   Knowledge of Security

This includes, knowing how to apply that technical theory, the understanding of security problems and the methods employed in using them to solve these problems. It also include the way to handle people and situation, and understand the practical approach, which obtains results calmly and efficiently, without embarrassment to the company or worsen industrial relations. Without a deep and purposeful study of the theory and practice of industrial security, a security officer cannot get his knowledge of security right. Practical works are only possible against sound theoretical background.

3.6   Training Functions of the Security Manager

In order to ensure maximum co-operation and co - ordination of translating common policy of the department, into a programme of action for the survival and growth of the undertaking, the security manager must do the following.

1   Provide his employees with information necessary for a clear understanding of matter that directly affect them, so as to secure and maintain their interest, develop loyalty and imbibe in them a sense of participation and responsibility.

2.   Adopt- regular training programmes for efficiency and professional growth, self-development and advancement.

3.   Establish an equitable basis of work allocation and impartial disciplinary rules that will create confidence and raise level of moral.

4.   Provide a sympathetic outlet for grievance so as to prevent frustration and avoid atmosphere of discord.

5.   Introduce rational and enlightened policy of retirement welfare scheme, to create a feeling of security of tenure.

6.   Establish scheme for consultation within and outside the department, so as to provide a means of exchanging information and viewpoints that will foster a sense of group harmony.

7.   Formulate security principles and policies for effective result, which must abide towards co-ordination of activities to achieve corporate goals objectives.

In addition to the above, the security manager must do the fpllowing.

a.   Organise the systematic supervision and patrolling of all boundary fences of the factory, storage areas, offices and buildings to censure the safekeeping of company assets.

b.   Make recommendations to management on all matters concerning security of company plant, buildings, /materials, personnel, and visitors etc, that need improvement. He will have similar responsibility in connection with property of any company employee (but where there is no legal liability on the company for such matters), only on an advisory capacity to help the individuals without obligation.

c.   Be responsible for the recruitment and the day-to-day administration of the security department/office, issue instructions on various aspects of security duties, and ensure the maintenance of a suitable standard of efficiency, and commitment. He must also take steps to provide them with

facilities to participate in a period of first-aid and security training, to keep their abilities in the field to the factory level, in consistence with the Factors Act CAP 66 and factories Decree No. 16 of 1987.

d.   Ensure that security staff are fully conversant with the operation of all equipment of the company, that such equipment are fully and adequately maintained, that satisfactory liaison is created and maintained, and fire occurring in the company is fully investigated and reported upon.

e.   Organise duties at all gatehouse to ensure that company's rules and regulations relating to entry and exit of employees, contractors, visitors and vehicles belonging to the company and other parties are observed. This will include the discretionary search of persons and vehicles.

f.   Cause such books to be kept in the gatehouse as, are necessary to ensure permanent record of commercial and private vehicle in and out of the premises with notation of purpose or load. He will also cause a day-to-day daily to be kept for reference purposes and such other records, as he deems essential for the efficient functioning of the security department.

g.   Responsible for the guarding of wages after receipt from the bank and during distribution to employees.

h.   Prepare annual estimate of expenditure to be incurred on the upkeep of the security staff/department, installations and equipment should be included in the annual budget.

i.   Keep in touch with development in mechanical, electronic and other aids to security, by maintaining contact with persons in parallel position in other companies and professional associations, through training and sharing experience in prevention of crime and the detection of offenders. The ability to train, organise and supervise the duties of security staff is required.

j.   The aims of setting up of security department are prevention, protection and preservation, effectiveness of the security department in carrying out these objectives depends on two factors namely: co-operation of the workforce and banking of the management.

k. The moment the workers realise that the company's security policy safeguarding their interest in the first place is by protecting them and their working environment, they would co-operate.

1. There must be a written standing order, which spell out the bounds of security authority, which is the company's directive to the security department and by which the company must stand absolutely.

l. The chain of command, naming the individual managers to whom the security department should report must be clearly spelt out. And, on no ground must anyone alter or vary any of the routine instructions without the consent of the management.

3.7 Qualities of Industrial Security Manager

Below are some qualities of an industrial security manager:-

i. Be bound by code of ethics or conduct of security practitioners.
ii. Possess relevant credentials. The components of credentials are-education, experience and or membership of a professional body like the Nigerian Professional Security Association, Nigeria Institute of Industrial Security, The America society for Industrial Security, etc. He must keep himself abreast of new ideals and new literature in his field. He should constantly be re-educating himself. He should endeavour to expand his own horizons.
iii. Be a well-informed business executive, and must posses five additional   important characteristics as follows:

- He should be constantly alert to possibility of error on the part of others. He should always check and crosscheck thoroughly.
- He should anticipate problems. He should be able to foresee, avoid and prepare for problems before they occur. He should posses the necessary experience and foresight.
- He must be action-oriented. He should be fast in studying problems, situations, and quickly make move to tackle them.
- He must be able to take decisions with confidence.
- He must be able to finish a job within a given deadline.

SELF-ASSESSMENT EXERCISE 2

Examine the two objective factors of effective security department.

4.0   CONCLUSION

This unit has briefly created the awareness of the basic security knowledge and Academic research. You are also expected to understand that the broad equipment of supervisory staff and security managers are too diverse to be adequately enumerated. However the fundamental aspect of security surrounding the functions of security manager, supervisory staff and security staff, is to ensure that compliances with programmes of action for survival and growth of the security department is adequately operational.

5.0   SUMMARY

It is interesting that all standards are set and there is constant flow of operational information and a regular check on performance against operating result, which provide room for quick response and adjustments.

6.0   TUTOR-MARKED ASSIGNMENT

1.   State five duties of security staff.
2.   State ten responsibilities of security supervisor.
3.   Illustrate the organisation chart of industrial security department.
4.   Differentiate between security knowledge and knowledge of security.
5.   Discuss some qualities of industrial security manager.

7.0   REFERENCE/FURTHER READING

Charles, A.S. (1998). *Effective Security Management*. London: Butterworth Heinemann Books Ltd.

Momodu, B. (2001). *The Basic Security Knowledge and Planning.* Lagos: Olucity Press Ltd.

Umar, S. (1997). *Security Operations Guard Force*. Lagos: Jo-Sekyson Publishers.

UNIT 4   PATROL PROCEDURES AND TECHNIQUES

CONTENTS

1.0   INTRODUCTION

Patrol may be defined as the act of watching, protecting or safeguarding a facility by moving continually around and through it. It involves walking or, riding a given route to observe the condition of the facility. The perimeter is an important patrol, as are warehouse areas, or open yard storage areas.

2.0   OBJECTIVES

At the end of this unit, you should be able to:

- detect and prevent fire outbreak
- detect and prevent criminal intrusion
- ensure company rules regarding safety and security are observed
- prevent automobile and industrial accidents in the premises
- detect and prevent damage and wastage to company properties

- identify and rectify vulnerable prints round the premises
- detect and prevent illegal disposition of subversive materials near sensitive areas.

3.0   MAIN CONTENT

3.1   Security Patrol Duties and Responsibility

The following duties and responsibilities are very crucial to every successful

Patrol man

a.   Ensure that the area is secured from intrusion and all gates and other entrances as prescribed are closed and locked.
Interior spaces must be checked to see that all doors, windows, skylights and vents are locked and secured against intrusion as well as possible damage from the weather.

b.   Turn-off lights, fans, heaters and other electrical equipment when its operation is not indicated.

c.   Check for unusual conditions, including accumulations of trash or refuse, blocking of the fire exits, access to fire-fighting equipment, etc.   Any such conditions if not immediately corrected, must be reported to higher authorities.

d.   Check for unusual sounds and investigate their source. Such sounds might indicate attempted entry, the movement of unauthorised personnel, the malfunctioning of machinery, or any other potentially disruptive problem.

e.   Check any unusual odours and report them immediately, if the source is not readily discovered. Such odours frequently indicate leakage or fire.

f.   Check for damage to doors, tracks or weight guards, in cases where doors have been held open by wedges, tiebacks or other devices.

g.   These should be removed and their presence reported at the end of the tour of duty

h.   Check for running water in all areas, including wash rooms.

i.   Check whether all processes in the area of the patrol are operating as prescribed.

j.   Check the storage of all highly flammable substances such as fuel, kerosene, volatile cleaning fluids, etc., to assure that they are properly covered and properly secured against ignition.

k.   Check for cigarette or cigar butts. Report the presence of such butts in no smoking areas.

l.   Report the discovery of damage or any hazardous conditions, whether or not they can be corrected.

m.   Exercise responsibility control over watchman and fire alarm keys, and keys to those spaces as may be issued.

n.   Report all conditions which are the result of violations of security or safety policy. Repeated violations of such policies will require investigation and correction.

6.1.1 Patrol System

Several systems of organising effective patrol are as follows.

6.1.2 Fixed Route System

This is the system whereby a security operative is detailed to patrol along a given route, and to be at a definite place at a definite time.

3.1.3 Semi-Discretionary System

This patrol system allows the security operative to be in a certain place, at a certain time but other than that, he patrols the place at his own discretion and is not tied to a definite route,

3.1.4 Aberdeen Patrol System

This system is normally adopted where and when the area or premises of the establishment is very large and there is shortage of manpower. The available staffs are usually conveyed in patrol van to a part of the area where they disembark and patrol for between 30 minutes and 1 hour, and are later taken to another part of the area to do the same thing continually until the duty hours are over.

3.1.5 Follow-Up System

This system is brought into use when the area is of moderate size and there is shortage of manpower. The available staff are made to patrol at distance of 100 meters apart of each other around the area continuously, until the expiration of the duty hours.

3.1.6 For Information and Further Action, Fifa, System

This system applies to warehouse only. In this situation two security guards are put in a place - each guard at a diagonal end of the building, where they would maintain vigilance for the duration of their duty.
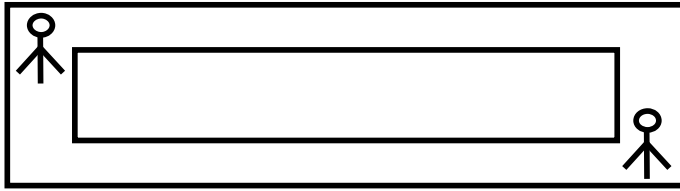
SELF-ASSESSMENT EXERCISE 1

Why is it necessary for a security guard to patrol his beat?

3.2   Rules for Patrolling Beat

The following rules are pertinent for beat patrolling:

a.   Ensure neatness and be neatly turned out
b.   Impress the workers and members of the public with your bearing and alertness.
c.   Never patrol in a hurry unless necessary.
d.   Patrol at a speed of about 3 kilometers per hour.
e.   Pay particular attention to property left without deterrence (closed property).
f.   Be polite when dealing with people.
g.   Be extra vigilant in the early hours of the morning 2 to 4 a.m.
h.   Do not idle away, gossip, sit or lie down or sleep while on patrol duty.
i.   Give special care to the aged and children.
j.   Pay careful attention to all properties and protection of lives.
k.   Do not leave your tour unless you are properly relieved.

3.3   Types of Patrol

There are broadly four types of patrols namely:

a. Day patrol
b. Night Patrol
c. Dog Patrol
d. Radio Patrol

3.4   Day Patrol

As the name implies, this is patrol undertaken during day time,

3.5   Duties during Day Patrol

a.   The patrolman must have knowledge of the business concern, how its products are made, which are vulnerable areas and who works in what departments or section.

b.   The patrolman politely uses friendly words here, a nod and a smile there, a short consultation with a supervisor and a briefing on the site from the security chief

c.   The patrolman uses his personality to create confidence for himself, to invite confidence from others, and to sell security as a service to the company and its employees.

d.   The patrolman takes a look at the fire appliances and the First-Aid Boxes, to see whether they have been used and replace empty or half to their normal places.

e.   It is the practice in some companies to allocate the appliances in a particular section of the premises to each day patrol guard as his special responsibility, so that each patrol guard develops a sense of pride to ensure that when required in emergency, he or his department or shift is not going to be found wanting.

f.   The patrolman warns visiting drivers about exceeding the speed limits, and to point out to them that the limit is not the order from the security department but the wishes of the workforce in the interest of safety.

g.   Extending patrols to employees' car park is good security practice, because it exhibits a security interest in the welfare of the employees and can have beneficial effects when keys left in cars are removed and kept for security reasons. Or when a telephone call is made to the driver that his lights are on or that he has got a flat tyre.

h.   Employees car parks are also a target for outside thieves. They should be deterred   by regular uniform patrol to car parks.

3.6   Night Patrol

This is somewhat more relaxed period but is known to be of more responsibility because it is during the night that company's trust in security guards integrity, sense of duty and conscientiousness come into reality.

3.7   Duties during Night Patrol

a.   The Patrolman now works alone in vast empty buildings and amidst silent machinery; sing his sense of sight, hearing and smell to their fullest extent to seek out possible intruders, dangers and defects.

b.   The patrolman decides in the circumstances whether there should be more light over and above the lorry parked at the other end or not, whether all the lights in the office block should be on or off, now that the cleaners have all gone.

c.   The Patrolman checks if cleaners have left the fire on when they made tea during working hours. He listens to running water that may have been left behind by unsuspecting cleaners and messengers.

d.   The Patrolman must suspect any car parked near the premises: Sometimes a couple could stay there to discuss. It could mean, I surveillance, activity by a suspected armed robbery gang. Get the car number and other descriptions.

e.   No company property should be removed by night unless on special instructions by the management, or during an emergency. No member of staff should be allowed into the premises at night except on special permission, or during an emergency. In an emergency or special permission the patrol security guard must follow the person into his office and possibly open and lock the office.

f.   The Patrolman should use the service of the walkie-talkie to transmit messages to the other side of the premises.

g.   The Patrolman should be particularly careful during night hours. Any unusual sound may represent the break-in of the warehouse. Do not take things for granted.

h.   Sleeping is dangerous. If you are awake and alert, you stand the chance of running for you dear life and go onto raise alarm in a safe place. This may be to deter more armed robbers.

3.8   Dog Patrol

Dog patrol is very effective only when the dog and the handler train together, and they are very familiar with each other. Dog could see, perceive odour and so they are sometimes more effective than the handler, especially at night. Dogs make patrolling more thorough, as one will discover a lot of security breaches with the dog. The handler must not repeatedly call the names of his dog at the beat or while on perimeter patrol.

3.9   Guard Dog

Dogs commonly used for security are the Rottweiler, Doberman pinscher, bullmastiff, German shepherd, boxer and the American pitball terrier. Among these, the most popularly used is the German shepherd, also known as the Alsatian. The Alsatian has hunting and guarding in its genes and it dates back to world War one, when the Germans used the dog to help rule the Third Reich. For solely security purposes,

Rottweilers are the best because of their body size, jaws and their aggressive nature.

Dogs are different range of security altogether and there are different kinds of canines that are trained just to fish out hoodlums.
Guard dogs need special care and attention. Canines are carnivores, but living amongst human beings has enabled them become slightly omnivorous. Training them to obey instructions and to attack intruders can revive the hunter's instinct in dogs.

All persons and organisations that provide dogs for security purposes for hire or reward should do the following:

a.   Keep a register readily available for all dogs in which details of each dog are recorded.
b.   Keep a log book for all hiring which should include the names of the dogs and handlers.
c.   Be adequately insured against all claims.

The following conditions must also prevail for an effective usage of dogs for patrol purposes.

i.   No dog should be used for security purposes unless it is fully and properly trained to such a standard.
ii.   Dogs should be kept in a healthy condition, property kenneled, fed and watered.
iii.   Every dog should be given close supervision at all times. (Preferable accompanied by a suitably trained handler).
iv.   Unless under the immediate control of the handler, dogs should be used only on premises or areas that are reasonably proof against escape and unauthorised entry.
v.   Docs should be transported only in vehicle which afford adequate protection against escape or injury to the dog.
vi.   Dogs should be in a compartment, separated from the driver.
vii.   Warning notices should be displayed where dogs are being used for guarding purposes.
viii.   Do not use or permit the use of a guard dog at any premises unless a trained handler, who is capable of controlling the dog is present at the premises, and the dog is under his control at all times, while it is being so used, except where it is secured so that it is not at liberty to go freely about the premises.
ix.   The handler of a guard dog should keep the dog under his control at all times while it is being used as a guard dog at any premises except:

a.   while another handler has control over the dog.
b.   while the dog is secured, so it is not at liberty to go freely about the premises.
c.   no one should use or per-nit the use of a guard dog at any premises unless a notice containing a warning that a guard dog is present ,is clearly exhibited at each entrance to the premises.

3.10 Radio Patrol

Today, the patrolman has exposure to several equipment. One of these is the two way walkie-talkie electronic Patrol Radio. The benefits to be derived from this equipment include as follows.

a)   It provides for a Patrolman to maintain contact with his colleagues in all site locations, and under conditions. He is no longer alone on patrol and therefore has the courage and feeling of security to go into situations which he would not attempt, but for his radio link.
b)   The patrolman can call up assistance without leaving the spot upon which he makes that decision. This may be a fire or accident, incident and observation or confrontation with intruders and/or suspects. It could be incident in which he is already injured or in personal danger; or it could be that he has come up on an unusual object demands investigation as a possible explosive device.
c)   It provides for the Patrolman to seek advice and guidance from a more experienced colleague or from his superior or manager. It is more efficient to take instructions on the spot through radio telephone than to expend time on a long tail back to the security office to obtain instructions.
d)   The radio provides for a supervisor or a manager to direct the movement of his patrolman to meet changing situations and to deal with incidents.

4.0   CONCLUSION

We have tried to discuss one of the most important aspects of security functions and responsibilities area which is patrol. It is therefore very vital for security operations to acquaint themselves with the meaning, importance and method of carrying out patrol duties for effective detection, prevention of Criminal activities and other offences against the coy interest.

5.0   SUMMARY

By the end of this unit students should be able to think that Security personnel on patrol must take their tours on routes or in areas assigned by the supervisor in charge. They must be fully aware of all policies and procedures governing their tour as well as those that govern the area patrolled. They must be alerted to secure the facility against any potential threat, and keep marauders and itinerant thieves from reducing the profit margin of the company.

6.0   TUTOR-MARKED ASSESSMENT

1.   Discuss the six routes systems of patrol
2.   Explain why night patrol is more sensitive than day patrol.
3.   List the four types of Patrol.

7.0   REFERENCES/FURTHER READING

Alla, O. (1997). *Security and Safety. Setting up Industrial Security Business*. Lagos: Spectrum Books Ltd.

Umar, S. (1997). *Achieving Guard force efficiently*. Lagos: Jo-Sekyson Publishers

UNIT 5   LOSS PREVENTION AND CONTROL

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Content
      3.1   Selection of Counter Measures
           3.1.1   Procedural Controls
           3.1.2   Hardware
           3.1.3   Electronics
           3.1.4   Personnel
      3.2   Personal Movement Control
      3.2.1   Protective Barrier
      3.2.2   Protective Lighting
      3.2.3   Intrusion Detection System
      3.3.4   Lock and key System
      3.2.5   Security Forces
      3.2.6   Security Control Post
      3.2.7   Security Education
      3.3   Hints on Security in Office
      3.4   Hints on Security at Home
      3.5   Hints on Security Outside Home (Public)
4.0   Conclusion
5.0   Summary
6.0   Tutor-Marked Assignment
7.0   References/Further Reading

1.0   INTRODUCTION

Every business enterprise or company is exposed to loss directly or indirectly, and the total of this loss is what determines the growth prosperity or decadence of the company.

Remember also, nobody for whatever reason imaginable will like to operate business at a loss no matter how tolerant and sympathetic the proprietor is. But surprisingly enough, very few companies are seriously concerned with loss prevention, and control efforts around their business which is part and parcel of security countermeasures

2.0   OBJECTIVES

At the end of this unit, you will be able to:

- pronounce that security personnel should be well trained and supported with reasonable security policies

- investigate suspicious or reported occurrences with depth and seriousness
- indicate search clause in the employees letter of appointment to avoid confusion when the need arises and to:

a) help you to use the techniques of under – cover investigation to detect any inconsistency, conspiracy or collaboration likely to occur around any business enterprise.

b) expose you to demonstration the use of security equipment to detect and apprehend criminals i.e. Alarm, CCTV system etc.

c) make you to be sure that perimeter fence, access points and gates or entrance are also property manned by competent security force.

d) assist you ensure that doors, windows, locks and keys are not broken and left to the advantage of an intruders or internal criminals.

e) help you try the use of Alarm on vulnerable and unprotected points.

f) assist you avoid employing local things or youth gangs into company employment or security department.

g) make you rotate security staff regularly to deter any undue familiarization with the internal employees.

h) expose you to consider very carefully the employment of two or more members of the same family in the same area where goods can easily be removed or hidden inside trash.

i) educate you on vehicles carrying trash are not parked near valuables or stores.

3.0 MAIN CONTENT

3.1 Selection of Countermeasures

There are four possible cures or countermeasures for every risk:

- Procedural controls
- Hardware (fences, gates, locks, keys, barricades etc)
- Electronic systems (access controls, alarms, CCTV, etc)
- Personnel

One of the important ongoing responsibilities of the security Director or manager will be to evaluate, select, and recommend appropriate deterrents for each significant risk from these four categories of countermeasures.

3.1.1 Procedural Control

Policy tells us what we must do, whereas a procedure tells us how we are going to do it. Procedural controls are intended to define how any activity is to be carried out in such a way as to prevent or expose any violation of policy (and attendant potential for loss).

This method is often the least expensive since it is often easy and involves little or no additional expense, to establish a controlled procedure as an uncontrolled one.

3.1.2 Hardware

Many loss risks can be significantly reduced by the simple application of some form of hardware, from a padlock on the company's gasoline pump, to a perimeter fence with adequate lighting. Hardware is most common in the average person's defensive strategy in his private life. Lockable suitcases, chains and locks to protect bicycles, bars or decorative screens on residence windows, front door peepholes, night latches, outdoor lighting constitute hardware. In the business environment, such physical protective measures may become more sophisticated, progressing to security containers (safes, lockable file cabinets, and vaults) and other equipment or devices. Still hardware is the second least, expensive among the four basic countermeasures.

In modern applications, security hardware is often combined with electronics; for example, a truck gate monitored by closed-circuit television (CCTV) that is electronically (and remotely) controlled, 01a fence whose protection as a physical barrier is supplemented by an intrusion alarm.

3.1.3 Electronics

In addition to CCTV, electronic countermeasures include such devices as automated access control systems, and the whole spectrum of alarms. These include intrusion alarms, motion detecting alarms, sound or vibration alarms, smoke detectors, heat detectors, and water--flow alarms. Electronic devices constitute the fastest growing category of security countermeasures. While initially more expensive both to purchase and install than procedural controls or basic hardware, they have become a fact of life for almost, all businesses large or small.

Alarms in particular were originally designed to replace the people who were previously deployed and utilised to provide precisely the same kind of alarm or warning service. Electronic alarms have proved to be more reliable than people for a number of reasons. They are less costly

compared to annual salaries of personnel required to perform the same function; they will not fall asleep; they are always on the job and they are honest.

3.1.4 Personnel

Ironically, the utilization of people as a security countermeasure can be the most efficient and effective strategy or, depending upon the circumstances, the poorest.

Because of the ongoing expense of personnel (not only for salaries but also for fringe benefits, vacation and sick leave, supervision, and replacement,) every effort should be exercised to cure risks whenever possible by means other than utilising people. The rule of thumb is to use people only in those areas where procedural controls, hare-ware, or electronics cannot be employed more efficiently.

Obviously, there are security functions for which people are the best and sometimes the only countermeasure. The greatest attribute of people, one which can never be replaced, is their ability to exercise judgment. In that capability lies a critical factor in the decision to use people. Wherever judgment is essential in carrying out a security function; people should be utilised. A common example might be the job of overseeing employees as they leave work in a production plant, by inspecting lunch pails and other containers. Personnel are essential for a variety of other roles that cannot be affected by procedures, hardware, or electronics. Among these functions are guard post and patrols, inspections, investigations, prevention of criminal attacks, maintaining order, and crowd control, etc.

SELF-ASSESSMENT EXERCISE 1

Electronic alarms have proved to be more reliable than people for a number of reasons "Do you agree?"

3.2   Personal Movement Control

Perimeter barriers alone in an organisation are not enough security. A positive personnel movement control system must be established and maintained, to preclude unauthorised entry. Access list, personnel recognition, security identification cards, and badge exchange procedure and personnel escorts, contribute to the effectiveness of movement control system.

An identification system should be established at each organisation to provide a means of identifying all staff and visitors. Provisions of

identification by card or badge should be included as part of the physical security plan.

3.2.1 Protective Barrier

Protective barriers are used to define the physical limits of an organisation. The use of barriers offers two important benefits to physical security posture:

a. They create a psychological consideration for anyone thinking of unauthorised entry.
b. Barriers have a direct impact on the number of security posts needed, and on the frequency of use for each post.

3.2.2 Protective Lighting

Protective lighting provides a means of continuing, during hours of darkness and offers a degree of protection, approaching that maintained during daylight hours. This safeguard also has considerable value as a deterrent to thieves and vandals, and may make the job of the saboteur more difficult. It is an essential element of an integral physical security Programme.

The principles on which protective lighting is based, is that it should enable guard forces, personnel to observe activities around or inside the installation without disclosing their presence. Adequate lighting for all approaches to an institution or organisation not only discourages attempted unauthorised entry, but also reveals person with the areas.

3.2.3 Intrusion Detection System

It is very important that all structures designed for the storage of firearms or cash are protected with an intrusion detection system, or be under close circuit television etc. Alarms must be enunciated at the security duty room from where a designated response force can be immediately dispatched. The intrusion detection system should remain in continuous operation during non-operational hours of the protected area, if they are to be effective.

3.2.4 Lock and Key System

The lock is the most acceptable and widely used security device of the basic safeguards in protecting organisations. Therefore, all containers, rooms, buildings and facilities containing vulnerable or sensitive items should be locked when not in actual use. However, regardless of the

quality, or cost, locks should be considered DELAY DEVICE only and not positive bars to entry.

There are quite a number of locks but the recommended ones are as follows.

a.   Key locks
b.   Conventional combination locks
c.   Manipulation resistant combination locks
d.   Other combination locks
e.   Relocking devices
f.   Cypher locks

3.2.5 Security Forces

The security force of any organisation provides the enforcement medium in the physical security programme. This force consists of person specifically organised, trained, equipped to protect the physical security interest in the organisation. This is the most effective and useful tool used for comprehensive integrated physical security programme.

3.2.6 Security Control Post

Security control room or post is a prerequisite and indeed, must be integrated with intelligence in the overall strategy in planning the defense of an organisation. The security post should co-ordinate policies and procedure for organisations physical security programme. It should also be responsible for administering and maintaining the programme, and for conducting physical security inspection such as ID cards and cars going in and out of the organisation or company.

The security men should carry out surveys as a part of the overall physical security programme. The security post should also establish and maintain a current priority list of critical activities and facilities within the institution or company.

3.2.7 Security Education

Any security programme or system designed to combat the security threats will prove ineffective unless it is supported by an effective security education programme. Security personnel cannot effectively accomplish their mission without the active interest and support of everyone in the establishment. Such interest and support can be secured only through an active security education programme.

The objective of security education programme include amongst others to acquaint all personnel with the reasons for security measure, and to ensure their co-operation. The assumption by unit personnel that they are not concerned with security, unless they work with classified matters or in a restricted area, must be overcome. It must be impressed upon them and be continuously reiterated that a locked gate or file cabinet does not constitute an end in itself, but is merely an element in the overall security plan.

A continuous programme should be presented to select audience (primarily supervisors and other key personnel on timely and applicable topics) to develop and foster a higher degree of security consciousness.

3.3 Hints on Security in Office

i.   Doors leading to offices must be properly locked and keys handed down in designated place when closing or leaving the office.

ii.   All appliances must be properly switched off before leaving the office

iii.   In a computer network, access to strategic information should only be granted to authorised users e.g. production data.

iv.   Sensitive information should not be published on the company's website to avoid information tapping.

v.   Computer usage in a network system must be pass-worded to restrict log-in.

vi.   Unwanted documents should be well destroyed if possible through shredding.

vii.   Restrict company's discussions to limited areas.

viii.   Faulty doors and windows should be reported promptly and followed up immediately.

ix.   Make a list of all valuable items in your office and check periodically

x.   Have recognisable and unique marks on all valuable items.

xi.   Avoid leaving your visitor alone in the office especially when there is money in your drawer.

xii.   Do not leave workmen, cleaners, hawkers etc, alone in the office.

xiii.   Avoid keeping shared keys under foot-mat or other places to avoid unauthorised duplication.

xiv.   Avoid monetary transactions, especially cash payment- in the office.

xv.   Make it a habit to cover up sensitive documents before admitting visitors to your office

xvi.   Lock up portable items of valuables when not in use

xvii.   Question every situation that appears to be a breach of security

3.4   Hints on Security at Home

i.   Do not live alone (a case study is the murder of the first Nigerian female pilot)

ii.   If you must need a house help, ensure that you demand for his or her photograph (full length) and passport size, written application with both his/her signature and finger prints and must provide guarantor(s). He/She must not habour strangers or friends in the house.

iii.   Ensure that security lights can be switched on and off from inside the house. It is also important to switch on the lights outside and switch off the ones inside the house. These arrangements give you an edge over an intruder.

iv.   Remove any object such as trees, stick, ladder, drum, etc close to the fence of your house that can assist intruder from gaining entrance into your house.

v.   Help to raise alarm if your neighbour is in distress, as this gives a general feeling of security among neighbours.

vi.   Demand for identification card from anybody claiming to be from water works, NEPA, NITEL, Estate services or security Personnel. Often armed robbers and tricksters usually impersonate as officials to commit crime.

3.5   Hints on Security Outside Home (Public)

i.   Endeavour not to count your money openly, or spraying at public functions such as marriages, burials, naming ceremonies, etc. It could be reasons why armed robbers trial you home.

ii.   Do not patronise strange women or strange men. They could be agents to armed robbers, or those dealing in Human parts. Do you want to die in pieces? Besides HIV/AIDS is real.

iii.   Avoid going out alone if possible.

iv.   Try to vary the timing and your route home. Do not create a regular pattern of going and coming home as this enables an attacker to know your movements and plan an attack

v.   If you suspect that you are being followed, enter any busy public place such as a restaurant or library, etc and call for assistance.

vi.   When traveling, ensure that your valuables are close by; as a matter of fact within reach. In short, sleep with only one eye closed.

vii.   Dump the habit of eating from people you do not know especially when traveling. You could be drugged.

viii.   It is very important you seriously observe the looks and movements of the occupants of a taxi or bus before entering. Often people recount, tales of how they lost valuables to hoodlums or thrown out of a moving taxi or bus.

ix.   Immediately you come out of a bank, do not board any waiting motorcycle or taxi; most are known to be agents to armed robbers.
x.   While in the bank, make sure you do not use your residential (home) address at the back to your cheque; instead use your official address especially when cashing large sums of money. Most times armed robbers' trial the owner home.
xi.   Avoid giving lifts to strange faces including uniformed security personnel.
xii.   It is advisable not to travel alone at night.
xiii.   If confronted by armed robbers, co-operate fully. Thereafter report to the nearest police station.
xiv.   Cooperate with bonafide security agents at checkpoints.
xv.   Tell somebody to whom you are going to visit; and when you are expected back.
xvi.   Be security conscious at all times. Think security, dream security and practice security.

4.0   CONCLUSION

It is imperative that every security system should have a set of define goals and responsibilities. This unit also emphasised on the need for security management to establish an organisational system to carry them out, and identify potential areas of loss and development, and install appropriate security countermeasures.

5.0   SUMMARY

We have been able to establish how the loss prevention and control were made possible cures for every risk. We concluded with the recommendation that the responsibility of the security director or management will be to evaluate and select the significant risk of counter – measures, for easy to remember if contacted (ERIC) operations.

6.0   TUTOR-MARKED ASSIGNMENT

1.   Explain the reason why loss prevention is important.
2.   Discuss the role of security protection in the office.
3.   Mention the possible counter – measures for every risk.

7.0   REFERENCES/FURTHER READING

Alla, O. (1997). *Security and Safety: Setting up Industrial Security Business.* Lagos: Spectrum Books Ltd.

Acha, K. (2003). *Security Manual.* Port Harcourt: Sakeche, Publishers.

MODULE 3

Unit 1   Basic Principles of Ethics
Unit 2   Security Policy and Design
Unit 3   Evaluation of Protection Programmes
Unit 4   Administration and Documentation of Security Records and Reports
Unit 5   Samples of Security Procedures for Access Control at the Gate

UNIT 1   BASIC PRINCIPLES OF ETHICS

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Content
        3.1   Meaning of Ethics
                3.1.1 Attributes of Ethics
                3.1.2 Concept
                3.1.3 Content
                3.1.4 Judgment
                3.1.5 Standards
                3.1.6 Values
        3.2   Security Ethics
                3.2.1 Sources of Security Ethics
                3.2.2 Religious System
                3.2.3 Philosophical System
                3.2.4 Cultural System
                3.2.5 Legal System
                3.2.6 Professional Codes System
        3.3   General Overview of Security Ethics
        3.4   Purpose of Professional Ethics
        3.5   Ensuring Higher Ethical Standard
        3.6   Standing Orders for Security Personnel
4.0   Conclusion
5.0   Summary
6.0   Tutor-Marked Assignment
7.0   References/Further Reading

1.0   INTRODUCTION

Ethic is derived from the Greek word ethos, and this refers to a person's fundamental or basic orientation towards life. The Latin translation of ethics is <u>Mos</u> or Moris. From Moris we have the word moral. Ever

since then, the word has attracted voluminous Literature, but with more universally accepted definition by writers in this field. Often, attempts had been made by a number of writers to draw a distinction between morals (What people do) and ethics (what they think they ought to do).

2.0   OBJECTIVES

At the end of this unit, you should be able to:

- define Ethic from Ethos and Morals from Moris
- summarize major attributes of ethics
- discuss sources of security Ethics
- mention various purposes of professional Ethics
- explain the factors of higher ethical Standards
- list many approaches of standing orders for security personnel.

3.0   MAIN CONTENT

3.1   Meaning of Ethics

Ethics is therefore a mass of moral principles or sets of values about what conduct to be. It may be specified by a written and unwritten set of codes or principles governing a profession (Steiner, 1975).

3.1.1 Attributes of Ethics

There are five major attributes of ethics that constitute the moral approach and consideration to a person's fundamental or basic orientation towards life. They are concept, content judgment, standard and values. However these are summarised as follows.

3.1.2   Concept

The field of ethics can be conceived as a discipline, science, study or evaluation.

3.1.3 Content

The subject matter of ethics is concerned with what is good or bad, right or wrong. Words usually encountered in discussion of ethics are true, fair, just, right and proper. Etc.

3.1.4 Judgment

Judgment is required to determine whether human action is ethical or not.   There are concerns over acts, not the motivation behind it. Behaviour and not its cause is that which is judged.

3.1.5 Standards

Judgment is based upon standards that are of course values.

3.1.6 Values

The final element of ethics is the set of values and criteria used as standards for judging human conduct.

3.2   Security Ethics

Security ethics is therefore directly related to the conduct of security practitioners. It is concerned essentially with the impacts of security decisions on people, within and without the organisation individually and collectively, in communities and other groups. Ethical behavior is a conduct that is considered fair or just, measured by ethical rules, and which must be obedient to valid government laws and regulations.

The argument further goes that security practitioners are human beings with ethical values that cannot be separate from their normal organisational lives. Therefore more and more security decisions should cover ethical and moral issues. This is in spite of the basic fact that broad ethical norms are fuzzy, there are rarely detailed rules of conduct; and where they exist, they are found to be contradictory and sometimes confusing. In any case, Nigeria Security practitioners, should be more ethical in their conducts and this conforms to the assertion that, a morally responsible security in particular situation that has clear idea of what values hold, ascendance over others in practice.

3.2.1 Sources of Security Ethics

There are five principal repositories of values influencing security practitioners and managers. These are religious, philosophical, cultural, legal and professional codes systems.

3.2.2 Religious System

 Most fundamental perception or conception of what is right or wrong in life is rooted in biblical morality. The society believes that moral values are of divine atheistic origin and often rest on atheistic foundation. Most

religions in their tenets emphasise that, the social responsibilities of people is to act in such a way as to contribute to the welfare of the society. Alternatively, men should not act to harm it (i.e. society) in any way.

3.2.3 Philosophical System

An important source of ethical conduct come from the views of great thinkers like Plato, Socrates, Aristotle, etc. all these men had a great deal to say about ethics. For example, Aristotle laid down the Golden Rule: "we should behave to friends as we would wish them to behave to us". Immanuel Kant (1724-1804) tried to find universal Laws of morality to guide men's conduct. Jeremy Bentham (1749-1832) developed a utilitarian system as a guide to ethics. This concept was perfected by John Stuart Mill, David Hume and John Locke in the nineteenth century. These great philosophers did develop standards of ethics, and their beliefs are measures of ethical standards in contemporary society.

3.2.4 Cultural System

The socio-cultural dimension includes the customs, norms, beliefs and values which characterise the environment in which the societal practitioner and organisations operate. These cultural factors have the dominant ethics of preserving the social system. Appropriate standard of security practice/conduct vary across cultures.

3.2.5 Legal System

The law is a confiscation of customs, ideas, beliefs, and ethical standards which society wishes to preserve and enforce. A web of law, regulations and court decisions encircles every security practitioner and manager. Some are designed to protect workers and consumers. Others are designed to make contracts enforceable and to protect property rights. Many are designed to regulate the behaviour of security mangers and their subordinates in organisations. There is relatively little that a security manager can do in any organisation that is not in some way concerned with, and often specially controlled by a law or regulation. The law cannot cover all ethical conducts

It has been observed to the dismay of security managers and organisations that the legal and legislative environment is confusing and full of loopholes, when it comes to interpretation, and ambiguous where two or more bodies are directly involved in the enforcement of any law, the internal jurisdictional questions have to be resolved first. Often this resolution takes time. These legal interpretations, ambiguities and bureaucratic entanglements usually make it very difficult for our

security managers to know exactly what course to take or what decision to make. Also, some security practitioners and managers have taken advantage of these loopholes to engage in unethical practices.

3.2.6 Professional Codes System

Professional codes are becoming a major source of ethical norms for security practitioners and managers. Three broad types of these codes have been identified. First are company creeds or philosophies, which are usually short, widely distributed and cover those basic philosophies that presumably govern the organisation. There is usually no standard format for creeds. Some of them are essentially economic statements, but many are basically codes of ethics.

The second types of codes are found in company operational policies, which set up guides to locate what have an ethical content. For instance, specific policy statements concerning such matters as procedure for hiring, promotion and firing employees; making decisions about suppliers and distributors, or handling customer's complaints, or security matters.

Third, security practitioners and managers are members of one association or industrial group or the other. Many of these professional, industrial or trade groups have codes of ethics which their members are expected to adhere to. Professional security practitioners are required to observe proper standards of professional conduct, whether or not the standards required are written in the rules or are unwritten. They are specifically required to refrain from misconduct, which is difficult to define precisely but which includes any act or default, which is likely to bring discredit on him, his professional body or the profession generally.

SELF-ASSESSMENT EXERCISE 1

Differentiate between Ethos and Moris.

3.3   General Overview of Security Ethics

Several general points can be made which include:-

- the professional security practitioner must possess diverse minds, competent abilities, proven achievements, and broad-based experience
- integrity is vital, synonyms for integrity include honesty, trustworthiness, uprightness, probity, rectitude, moral soundness, etc.

- professional security practitioners must not only be people of integrity, they must also be seen to be so
- when a professional security practitioner has ethical difficulties or unsure of what course of conduct to followed, he should consult his professional body or take legal advice. If in doubt always seek advice.

3.4   Purpose of Professional Ethics

The need to have public confide once and promote the profession, has forced professional bodies all over the world to establish the code of Ethics for the members of the profession.

In any association, there must be set of rules and regulations that are binding on members of the association. Examples are Nigerian Bar Association (NBA), Nigerian Medical Association (NMA), Institute of Chartered Accountants of Nigeria (ICAN), Institute of Management Consultants (IMC), Nigeria Institute of Industrial Security (NIIS), etc.

These codes of ethics are established to do as follows:

- Guide members in the practice of the profession
- Promote the security profession
- Establish confidence on the work of security practitioners
- Establish standards of practice for all the members.
- Protect the members and the profession in the case of legal action.
- Enforce security practitioners to be competent.

3.5   Ensuring Higher Standards

1. One of the major problems of ethical codes is their lack of active support by top management. Top management must make a commitment to think about and improve the ethical conduct of security practitioners and other employees in the company. Part of this commitment is an obvious preparedness to be ahead of others in equitable and just treatment of interest of persons, group.

2. Example of better than precept is a popular saying that goes," since employees' behaviour is generally influenced by the actions of the boss, top management must take the lead by setting good example of high ethical conduct." There is no point for top management to ask their subordinates to eschew unethical practices, while they chew them with relic.

3.   The two most outstanding factors that can bring about higher ethical standards are:

a.   Public disclosure and publicity.
b.   Increased concern of a better informed employee and public.

4.   According to Koontz et al (1980) "To make ethical code effective provisions must be made from their enforcement". Unethical security practitioners and managers should be responsible for their actions. This means that privileges and benefits have to be withdrawn and sanctions have to be applied.

3.5 Standing Orders for Security Personnel

It is important to conclude our discussion of ethics with standing orders for security personnel. They are as follows:

a)   The security practitioners must not neglect, or without any sufficient cause omit to promptly and diligently discharge his required task while at work.
b)   He must not leave his place of duty without due permission or sufficient cause.
c)   He must not knowingly make or sign any false description. This is confidential to any employee or client past or present
d)   He must not without due and sufficient cause, past or present. Employee or client
e)   He must not without authority, divulge any matter which is confidential to any employee or client past or present.
f)   He must not corruptly solicit or receive any bribe or other compensations from any persons or fail to account for monies or properties received in connection with employer's company.
g)   He must not be uncivil to persons encountered in the case of his work or make unnecessary use of authority in connection with the information that will be discharged from the employer's company.
h)   He must not act in a manner reasonably likely to bring discredit upon the employer, a client or fellow employee.
i)   He must not feign or exaggerate any sickness or injury with a view to evading work.
j)   He must not wear the employer's uniform or its equipment for illegal duties.
k)   He must maintain proper standard of appearance and deportment while at work.
l)   He must not work while under the influence of alcohol or consume any alcohol while at work.
m)   He must not have been convicted by any criminal offence.

n)   He must not neglect his hazard hours – from 2 to 4 a.m.

o)   He must endeavor to be the kind of security practitioner management wants him to be.

p)   He must not argue or encourage unnecessary argument in the cause of his duty

q)   He must maintain the uniform provided him by management, unless otherwise directed.

r)   He must be exposed to fire and first-aid training at agreed intervals.

s)   He must not unnecessarily familiarise himself with members of the work force

t)   He must not lose his temper at any time while on duty.

u)   He must promptly respond to any emergency call in the premises of his employers.

v)   He must be very observant of criminal activities

w)   He must understand basic principles of investigation

x)   He must possess a character that is above board and present himself as a responsible and disciplined officer at all times.

SELF-ASSESSMENT EXERCISE 2

This unit has acknowledge the three broad types of professional code which are becoming a major sources of ethical norms for security practitioners and managers, "Do you agree?".

4.0   CONCLUSION

This unit highlighted the definitions and concept of security ethics. Sources of the security manager's ethos were identified and briefly discussed. We discussed the general overview of security ethics, basic factors, and purposes of professional ethics. Finally, few ways by which ethical behaviour can be improved were given. Also given were standing orders for security personnel.

5.0   SUMMARY

We are aware that enforcement of ethical codes may not be an easy task, but the mere existence of such codes and the feelings of their enforcement, can increase ethical behaviour.

The employees and public must know how and why the organisation's security operates decisions are made, roles of the organisation in socio-economic development of the society, and probability of institutionalising or executing a social point of view.

6.0   TUTOR-MARKED ASSIGNMENT

1.   List only ten standing orders for security personnel
2.   Mention six purposes of professional ethics
3.   Discuss the major attributes of ethics

7.0   REFERENCES/FURTHER READING

Brown, L. S & Swiznick, P. (1968). *Sociological Paradigms and a Test with Adapted Readings.* Texas: Harper Collins Publishers.

Gilbert, F. & Lilian, G. (1972). *Industrial Psychology.* Cambridge: Harvard University Press.

Koontz, N. (1980). *Enforcement of Ethical Codes.* New York: Paeger Publishers.

Steiner, S. (1975). *Principles of Ethics Governing a Profession.* California: Mayfield Publishers.

UNIT 2   SECURITY POLICY AND DESIGN

CONTENTS

1.0   INTRODUCTION

It is the aspect of security operation which constantly breads contempt, resentment antagonism and conflict in any, responsibility center. In order to resolve these problems and clear away doubts between the security operatives, proprietors and employees, a clear sighted security policy becomes imperative. However, despite the increasing waves of crime around businesses today, it is very unfortunate to observe that many organisations operating in sensitive business premises do not have a single security policy to guide the conducts of employees and the rules of security operations. And because of this neglect, quarreling, mud-slugging, conspiracy and lawlessness will become the order of the day around such organizations, between security operative who are trying to perform their legitimate duty by blocking all avenues of committing crimes, and the disgruntled employees trying to avert such effort and commit crime. Worst of all, some members of the management not only allow such saga to happen but take delight at the unfortunate episode.

2.0   OBJECTIVES

At the end of this unit, you should be able to:

- state the role of security operatives in any protected premises
- state the role of the policeman
- explain why criminals do not like police presence.

3.0 MAIN CONTENT

3.1 Definition of Security Policy

Literally, security means protection and preservation of lives and property in their totality against assaults, 'sabotage, loss, fire, frauds damage or unnecessary wastage in any given premises. However, security duties cannot be effective and complete without the active participation of the guard force or police force in patrol duties, to access control at gates and other strategic entrance, weight bridge operations searching vehicles and employees, conducting investigations, preventing fire out - break, protection and control of process secrets, financial data, confidential information of vital interest to the company through a uniform and unbiased application of security rules and regulations in offices and the premises in general.

3.2 Policy Formulation

The formulation of security policy is the sole responsibility of management at board level. And such task should be done in an atmosphere of confidence, trust and the general interest of protecting the lives of employees, customers and visitors against all criminal assaults, as well as, the protection of company's properties against all range of crimes. This will be supported by setting parameters within which security operational powers, procedures and conducts of the operatives will look like, with emphasis on the continuous support, good-will and cooperation of all and sundry on the organization, for the success of security operations. Mechanism of interventions by the management from time to time, to serve the prestige of the security policy or constitution and check mate lawlessness, should be created and reposed in the hand of a competent management staff, This staff must not only render explanations in the event of adverse security breach but will, from time to time, be called to account for the general security and safety of the organisation. It is because of these responsibilities that management staff responsible for the formulation of policy, should know the extent and parameters within which policy should operate, to provide cover for the organisation.

3.3 Policy on Security

Security is the be-all and end-all of all protection measures. Without security, there is no protection and in the absence of protection, crime lawlessness, and obstructions will prevail.

Therefore, policy on security has all the paramount importance in asserting protection. There are the following laid emphases.

1)   How the security operations should look in general in the organisation.
2)   How the security department should discharge its functions.
3)   How security should approach all security matters i.e. searching, investigations arrest, patrol, inspections etc.
4)   How employees should view security roles and obey the norms guiding their behaviours in relation to daily security operations in the organisation.
5)   How the security hierarchy will be and the methods of reporting, as well as the accepted channels of communication and sequence of command.
6)   The limit and extent of powers to be conferred on security managers, supervisors, co-coordinators and the shop floor security operations.
7)   The colour of uniforms, equipment and other working tools to be used by the security department and operatives.
8)   The method and yardstick of controlling, auditing and inspecting security operations to improve efficiency.
9)   The appropriate techniques, methodology and response capability and options to new crime waves and threats to industry and commerce in general, and how such response will be measured in accordance with the available and limited resources

SELF-ASSESSMENT EXERCISE 1

Policy on security has all the paramount importance in asserting protection "Do you agree?"

3.4   Policy on Recruitment

Among the challenge facing commercial and industrial organisations today is staffing the security department with honest, sincere and hard working security staff. This has become a source of concern to many organisations because of numerous breaches of security with the covert and overt participation of security staff. However, despite such incidents, some companies are headless about formulating policy on recruitment, if not ridiculous to employ security staff and wake up one day to discover that the security staff has decisively dealt with the organisation. Such incidents do occur whenever careless and disorganised recruitment exercise is carried which leaves so many loopholes, to the advantage of the security staff who may be a person of questionable character. Policy on recruitment is aimed at defeating such lumbers in its totality. The acceptable procedures on policy on recruitment are as follows.

1)   Define the criteria for recruitment, selection, interview and vetting of security staff before committing them to organisations services.

2)   Criteria for checking the suitability physique, health condition (medically fits) and moral attachments of the applicants.
3)   Identifying a reliable source of recruiting corrupting and experienced security   force to staff the department.
4)   Standards and criteria for training induction and deployment of the staff according to accepted operational standards
5)   Criteria for education, retirees from any of the armed forces and not up to 70 years of age.

3.5   Policy on Employee Dishonesty and Crimes

Certain sections of labour acts and trade unionism have the prerogatives to reverse the dismissal of employees when the circumstances surrounding the punishment are discovered unfair.

In addition to these, grounds for dismissal are carried out and can be challenged by employees in a court of law, which is capable of scandalising and tarnishing the image of a reputable company.

And it is also capable of <u>destabilising good industrial relation between the rest of employees and the organisations.</u> Apart from all these, some employees when dismissed may resort to dangerous maneuvers i.e. ARSON Attacks, ASSASINATION PLOT etc. against the company, executive or managers in an attempt to settle an embittered score. It is in a bid to avoid all these unmitigated embarrassments that a clear-cut policy on employee dishonesty and other crimes should be formulated.

Thus will include the following statements:

1.   The definition of employee dishonesty and the extent to which it can warrant the award of punishments.
2.   Measures and manner of investigating employee dishonesty and other crimes.
3.   Appropriate yardstick for awarding punishment commensurate with an alleged offence.
4.   Compensatory measures for wrong done to wrong victims.
5.   Extent to which police and regular count will be involved in-awarding punishments.
6.   The particular department for dealing with employee dishonesty and its extent of Authority in dealing with dishonest employees.
7.   The powers and extent to which arrest can be instituted by whom and by which department and according to which portion of the company policy.
8.   The methods with which stolen properties can be recovered and returned to the company.

3.6   Policy on Retrenchment

Retrenchment in any organisation is a risky and sensitive exercise which security policy initiatives must pay attention to. Apart from its potentiality to spark off protest, demonstration and violence, retrenchment exercise can produce an atmosphere where deadly conspiracy could be hatched against the company and its executives. In view of these immense implications, policy on retrenchment should be stipulated with specific instructions to the security department, and the roles the security department will play during such exercise. The policy on retrenchment should clearly define these items.

(1)   What role the security department should play.
(2)   How the security of retrenchment information should be protected against leakage.
(3)   How the management should react to any volatile and hostile situation with direct consequences to security of lives and properties, in the event of information release or leakage of the retrenchment exercise.
(4)   The extent of contingency and emergency preparations against violence and precipitous confusion.
(5)   Who will take charge of security operations in an extraordinary situation?
(6)   To what extent law enforcement agencies will be involved in controlling a volatile situation.

3.7   Policy on Searching

Apart from its legal implications, searching employees in any organisation has been the source of frictions, hatred and enmity between the security department and the employees. Dishonest employees will not hesitate to capitalise on this confusion and start paralysis of initiatives to commit crimes. Neglect of search operations naturally creates the temptation among employees to conceal the concealable, and get away with it. At least, the employee will say it is company's property and it is our sweat, and a company is always a big ocean where everyone, if opportuned, can dip his cup provided he is not caught. It is this misconception of reality which instigates most employees to try to dip their cups into the company's ocean wealth. In another realm, others may see search operations as an exercise which doubts their sincerity and therefore an insult on their person. They always resent and hate it but how sincere and honest they can be to their conscience and resist the temptations to steal is what cannot be ascertained. In order to avoid all these embarrassments and confusions, it is necessary to institute policy on searching that will be enforced across the organisation.

And it will be very effective when management staffs first and foremost surrender themselves to the exercise. However, policy on searching school clearly explains as follows.

1. The inclusion or insertion of search clause on the terms and conditions of service so that no employee will view and resent against searching as illegitimate exercise.
2. Extending specific powers to security department on the routine need of searching's the extent to which search exercise can be conducted.
3. Communicating temporary or permanent notice of search operations through appropriate authority to all employees.
4. The specific actions to follow if employee refuses to submit himself to searching.
5. The specific actions to follow if employees are found with incriminating property.
6. At which points and exits searching can be legitimately conducted.
7. The extent to which arrest can be instituted and how police may be invited.

SELF-ASSESSMENT EXERCISE 2

Why is it necessary to institute policy on searching and enforce it?

3.8   Policy Implementation

Formulation of policy is one thing and the implementation of the policy according to policy recommendations and procedures is another. Some companies have the policy formulated adequately covering all aspects of securing affairs, but unfortunately the policy is either not implemented completely or is repeatedly violated and therefore becomes ineffective. This syndromic development has been contributing to the emergence of confusion in policy implementation in many organisations. And to avoid these, policy implementation should lay the following emphasis:

(1) It should be clear - cut, incisive and its implementation should not easily be manipulated by someone or others for personal or selfish interest.
(2) It should not carry an iota of favoritism, insincerity and dubious dealings.
(3) It should reflect the overall interests of the organisation irrespective of who does what.
(4) It should be enforced across the whole organisation
(5) It should be subjected to review periodically

(6)   It should reflect fairness, justice and aim at balancing security, safety and good industrial relations

(7)   It should be broad - based with the participation and representation of other organs in the organisation while undergoing formulation.

4.0   CONCLUSION

Let us examine these scenarios as a case study. In one episode in October 2002, senior employees collaborated and went away with N700, 000: 00 (Seven hundred thousand naira) from the vault of a bank, in an attempt to implicate security operations. This happened after series of confrontations between the security operatives and the disgruntled employees who constantly refused the security operatives to search their vehicles, the bank management affably doing nothing to stop the lawlessness. And when investigations were carried out, the so-called trusted bank staffs capitalised on the no – search opportunity to surreptitiously cart away the money in a phony sports bag. This is one of the dangers to which both the security operations and the businesses are exposed to daily in the absence of a clear-sighted and responsible security policy.

5.0   SUMMARY

It is a pity to also observe that see many so-called professionals and corporate managers of today do not know that they have serious responsibility for security. Whenever their employees misbehave in matters with grievous security implications, they revert to inaction, divide and rule gaming believing that security is not essential to the growth and prosperity of the organization. That their employees are honest, if that assumption is anything to go by, we should not be seeing executives and managers in police cells, facing tribunals with long sentences today. Nobody is perfect and not all consciences are clear. In any business environment, the direct involvement of every management grand, from the managing director down to junior managers in the policy formulation and control, becomes imperative if business must escape the embarrassments of crimes and crisis. Any act of negligence at the management level, will surely be reflecting in the attitudes of all employees, including the security operatives, to the extent that all security operations will be pointless rabble of confusion and pot of conflicts.

And for any business to be safe and survive, security operatives must be given free hand to operate in accordance with a clear-sighted and responsible security policy, which guides all conducts of employees including the security operations themselves.

6.0   TUTOR-MARKED ASSIGNMENT

1.   Explain the meaning of security policy.
2.   State the Authority that is responsible for the formulation of security policy.
3.   Discuss the legal implications of policy in searching.
4.   Compare and contrast destabilising good industrial relationship between the remaining Employees and the organisation.

7.0   REFERENCES/FURTHER READING

Osuala, E.C. (1982). *Introduction to Research Methodology.* Onitsha: African Publishers.

Umar, S. (1997). *Achieving Guard force Efficiency.* Lagos: Jo-Sekyson Publishers.

UNIT 3   EVALUATION OF PROTECTION PROGRAMMES

CONTENTS

1.0   INTRODUCTION

Evaluation of protection programme is associated with loss and risk analysis in security operations. However, they are dangers and suffering, harm or losses through unnecessary exposures to risk-bearing.

2.0   OBJECTIVE

At the end of this unit, you should be able to:

- establish the possibility of every company being exposed to one kind of risk or another. E.g. burglary, fire, fraud, robbery, etc.

3.0   MAIN CONTENT

3.1   Causes of Industrial Loss

Industrial loses do not just course they are caused. The basis of security is the need to know the loss prevention and reaction in industrial security. Therefore, the loss prevention specialists have analysed the causes which include unsafe attitude or act, unsafe conditions, and unsafe response respectively.

3.2   Unsafe Attitude or Act

Behavior or actions that expose life and property to danger or security risk due to error, negligence, carelessness etc; for example, personal

97

protection, equipment or right ,tools provided for a factory worker but he refuses to use those items and gets injured, ignoring casino, etc.

3.3   Unsafe Conditions

State or circumstance or place not providing good protection or not free from danger or security risk e.g. overloading or crack of walls, or any other damages in the factory, which can cause losses to the company.

3.4   Unsafe Response

Environment induced actions, events, happenings, etc, that can result in losses to the company, e.g. adverse legislation, riot, war, natural disaster like earthquake etc.

3.5   The Triangular Theory of Industrial Loss

We can now sum that unsafe act resulting to unsafe conditions, or unsafe conditions, resulting from unsafe act, or unsafe response resulting from unsafe conditions or unsafe conditions resulting to unsafe response which cause unwanted, sometimes unrecoverable losses-

DIAGRAM 1. TRIANGLE OF LOSS

1. HE-HUMAN ERROR
2. UC-UNAVOIDABLE CIRCUMSTANCE
3. UH-UNFORSEEN HAPPENING
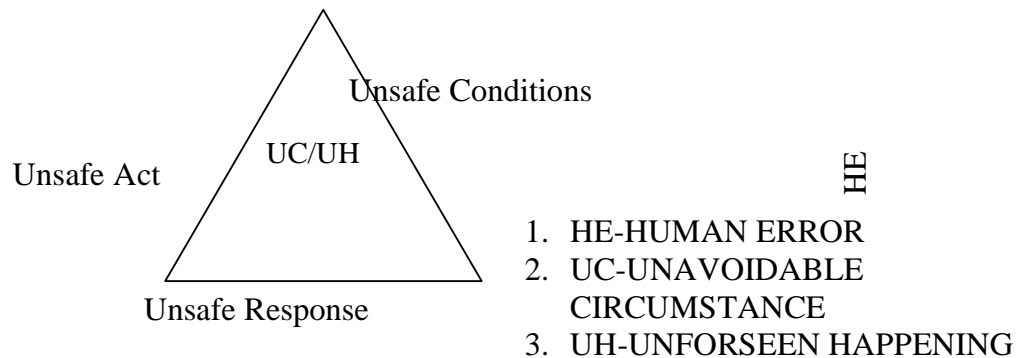
SELF-ASSESSMENT EXERCISE

Industrial losses do not just course they are caused "Do you agree?"

3.6   The Industrial Security Environment

The security system does not exist in isolation. It operates within a larger environment, which has physical, economic, political, social, legal, cultural, moral and technological dimensions.   The security managers have to operate within the framework established by the

environment.   Environmental factors can and do affect security operations. These impacts could be favourable or unfavourable. As such, successful industrial security managers must be aware of their environments, know their possible impact on their activities, and adapt effectively to avoid unwanted or unrecoverable losses.

The diagram below shows the totality of the environment in which the security system operates. The reversible arrow connecting the security system with each of the environmental sub-system portrays the reciprocal nature of the effects which environmental factors have on the security systems and vice-versa.

DIAGRAM 2. INDUSTRIAL SECURITY ENVIRONMENT

Physical

Technology   Economic

Moral   The
Industrial   Political
Security
System

Cultural   Social

Legal
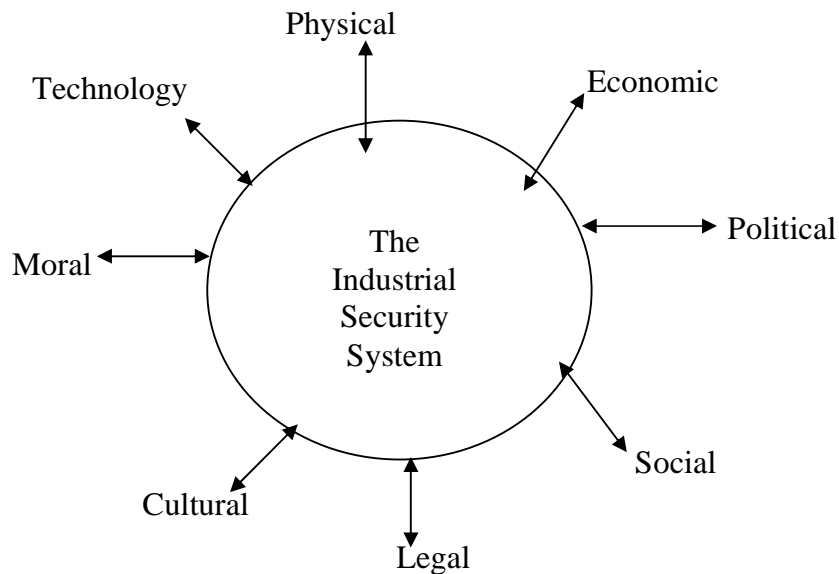
4.0   CONCLUSION

This unit has carefully explained that in view of these dangers, it is very necessary for security operatives whose role is to prevent losses to business, to know what constitutes a risk and how such risk can be analysed as well as avoided.

5.0   SUMMARY

In this unit we have analysed the general possibilities of causes of industrial security loss. And apart from these possibilities, buildings and machineries are daily exposed to arson and sabotage which can send a company parking.

6.0   TUTOR-MARKED ASSIGNMENT

1.   Explain the causes of loss in security.
2.   Describe the diagram of industrial security environment.

7.0   REFERENCES/FURTHER READING

Alla, O. (1997). *Security and Safety. Setting up Industrial Security Business.* Lagos: Spectrum Books Ltd.

Fisher, R.J. & Green, G. (1986). *Introduction to Security Management and Planning*. New York: Paeger Publishers.

UNIT 4   ADMINISTRATION   AND   DOCUMENTATION OF SECURITY RECORDS AND REPORTS

CONTENTS

1.0   INTRODUCTION

Students in this course will apply principles of management to security administration and documentation of records and reports. Despite the anticipation and record of criminal incidents, there are many understandings to the nature of threats posed, which is part of information system and business continuity.

2.0   OBJECTIVES

At the end of this unit, you should be able to:

- state the principles and issues in security administration, records and reports of events
- describe and demonstrate the relationship between importance of security records and justified rules of keeping records, in case of eventuality as they relate to private, government and business
- Apply research –Oriented approaches, case studies and the use of situation analyses as appropriate in the study of security administration and documentation.

3.0 MAIN CONTENT

3.1 Definition of Security Records and Reports

Apart from the anticipation and records of criminal incidents, there are several reasons why security operatives should keep and maintain records of events in their area of responsibility.

Accurate and timely account of events provides both hind sight and fore sight to security departments and in the period of uncertainty and confusion, such records will help clear and exonerate doubtful matters.

The discussion in this lesson is to provide vital and necessary information about security record and reports.

3.2 The Importance of Security Records

Keeping and maintenance of security records and reports is as important as the entire force orations as a whole, and in their absence, security duties will not be as credible as it should be in times of serious trial. Some of the importance of security records is listed as follows.

i.   Records are necessary to keep full information and facts about security incidents, instructions, and performance of the guard force, cases of arrests and other vital facts during security operations.

ii.   Security operatives on duty do not inspire respect and confidence if they could not produce accurately recorded happenings on request, especially when they resort to guessing or had not recorded the incident

iii.   Records are necessary in handing and taking over of duty to clear away doubts during incidents of theft, where lack of records will create confusion as to who lost what and when. Remember it must be physically handing and taking over exercise and not on trust or compromisation

iv.   Recording of incidents, if accurately written will help the effort of investigations in identifying and knowing how incidents happen.

v.   All incidents should be recorded forth with during security operations. And it will be ridiculous, if not funny when a security operative has to start recording incident 24 hours after the incident has taken place.

3.3   Types of Records

Generally, there are four types of records in security practice. It is in these written records that all events of security significance are daily recorded and kept. These records are:-

1.   **Register: -** These are records used to keep a comprehensive register of items or events for the purpose of reference. Under these are numerous registers sub divided as follows:-

(a)   Visitor Register
(b)   Key Register
(c)   Lost and found property registers
(d)   Alarm test register
(e)   Borrowed tool register
(f)   Employee search register
(g)   Vehicle search register
(h)   Incoming mail register
(i)   Outgoing mail register
(j)   Attendance registers

2.   **Books: -** These are records used to record and keep a particular message, instructions, check list or reference for numerous security purposes. They are sub divided into:-

(a)   Duty occurrence book
(b)   Security equipments service and repair log book. Telephone
(c)   Message book
(d)   STD code book.

3.   **Forms: -** These are records in security practice used to record, keep or issue out instructions, advice, direction, for various purposes.

These are the folic,-wing:-

(a)   Industrial accident report form
(b)   Fire report form
(c)   Vehicle accident report form
(d)   Lost and found report form
(e)   Visitors pass form
(f)   Way bill and gate pass forms
(g)   First - aid treatment forms

4.   **Cards: -** These are records used to keep a permanent information and record for easy reference- Cards arm sub divided into:-

(a)   Driver's card

(b)   Visitor card
(c)   Identity card
(d)   Staff access card or card reader

SELF-ASSESSMENT EXERCISE

Is security records a report or an information? Discuss.

3.4 Rules of Keeping Records of Events

There are certain rules to strictly follow by security operative while recording events in the security records. Some of these rules are as follows:

1.   In the case of arrest, full names of 'the suspect age occupation and his physical descriptions should be recorded. Other information will include the time of the arrest, reasons for the arrest and reference to properties recovered

2·   There must be no additional writing in between written lines. Written pages must not be removed or torn away in order to make fresh entry.

3   If there is error in a recorded incident the correct procedure to follow is to draw a straight line across the erroneous entry and record the correct fact.

4,   Records should be meticulously kept and all abuses should be avoided.

5.   Records kept for the purposes of record must be fully utilised and used for such purposes, because it is not predictably possible for the security staff to know when question may arise in respect of a recorded event. The instant provision of such records on request to either the management or the court will inspire confidence, integrity and reliability of the security department and its activities.

6.   Records should be serially numbered in sequence and all entries by the user should be in chronological order, according to date and time. The accuracy and order of entries will justify its authenticity, in legal proceedings.

7.   Erasure or fresh insertion of entry will raise implicating suspicion. Tearing of pages or any other alteration of entries should not be allowed to happen; else the entire note book will be seen as a pack of forgery.

8.   Delayed entry of events or incident normally results in the severe criticism of the security officer in court as to why the entries were made belatedly.

9.   To crown it all you must ensure that entry should be made as promptly as possible provided the incident is confirmed.

4.0   CONCLUSION

In this unit we have learned that students will focus on security administration and documentation procedures, and maintenance of records for the safe custody and preservation of information, in case the need arises for easy reference.

5.0   SUMMARY

At the end of this unit, we have been able to provide vital and necessary information about security records and reports.

6.0   TUTOR-MARKED ASSIGNMENT

1.   Explain the meaning of security record and reports.
2.   Compare and contrast the importance of security records and the rules of keeping records of events.

7.0   REFERENCES/FURTHER READING

Charles, A.S. (1998). *Effective Security Management.* London: Butterworth Heinemann Books Ltd.

Braimoh, A. (2001). *The Basic of Security Knowledge and Planning.* U.S.A: New world Press.

UNIT 5   SAMPLES OF SECURITY PROCEDURES FOR ACCESS CONTROL AT THE GATE

CONTENTS

1.0   INTRODUCTION

In order to effectively control and monitor the movements of both visitors and internal staff, physical access control is necessary. The essence of access control in a responsibility area is to create an environment of security consciousness. This is done by establishing guard posts in virtually every strategic entry points to screen, question, watch and direct visitors and employees in the premises. Doorways, gates, lobbies, lifts, staircases, hallways, fire exit etc are vulnerable points where intruders can readily find very easy to access restricted rooms and area in offices. However, the strategic importance of each access point is determined by security interests. While some accesses are more important, others are not because the penetration of one access point will wreck less security havoc than another. However, all access points are very important and should be taken care of.

2.0   OBJECTIVES

At the end of this unit, you should be able to:

- explain what is meant by Samples of Security procedures for Access Control at the gate
- describe the processes and types of Access Control
- state why the words QWQS is very necessary for questioning the visitors as a security officer?

3.0 MAIN CONTENT

3.1 Physical Access Control

Physical access control is intended to check the following procedures:

1)   Illegal entry or unauthorised intrusion of persons into protected areas.
2)   Detect aim less wanderers in the office environment or company premises.
3)   Interrogate visitors and provide assistance when necessary
4)   Identify internal staff, for security purposes.
5)   Detect the deposition of subversive containers or carriages by sneak-in and deception entry criminals.
6)   Control crowds and visitors during peak business hours.
7)   Dis-arm visitors carrying offensive objects into office environment or company premises for security reasons.
8)   Maintain law and order by arresting trouble makers in the building.
9)   Keep fire exits and escape routes clean of any obstacles in case of emergency.
10) Screen deliveries i.e. Parcels, letters, bags, for security purposes.
11) Impose company's security policy at access points.
12) Control the opening and closure of access doors.
13) Ensure the privacy of employees and employers during working hours.

3.2 Types of Access Control

The nature and usage of building or premises determines the type of access control to be effectively used. However, the combinations of all types of access control will pay higher security dividend than one. In this case, there are three types of access control.

1. Visitors Access Control

In this type of access control, the problem of security starts with people because problems arises out of interaction, and intermingling of people of various shades and characters at different levels in the company. Visitors in this case can be classified into:

a)   Contractors
b)   Subcontractors
c)   Vendors
d)   Ex-staffs
e)   Non-staffs.

It is therefore very vital to control the access of this group of people by the introduction of:

- guard-post at every access-point to check their entry and exit
- visitors card access system to tag and distinguish between visitors and staffs of the company. so that aimless wanderers can be identified and restricted
- visitors-registration system to record such visits according to date, time, name, address and the purpose of such visits, so that investigation effort can be rewarded by referring to records of visitors whenever there is potential penetration or security breaches
- telephone-call system in order to establish instant communication with the persons the visitor claim to come to see especially when there is suspicion about the character seeking for access.

2.   Vehicle Access Control

Because of the manner of how cars are used to remove valuable properties from premises or how cars are stolen, and how terrorists use vehicles to attack targets with bombs by either driving straight into the premises and leave the bomb inside the car to detonate itself. There is the need for effective car access control measures. This can best be achieved by the introduction of:

a)   Vehicle Access Card/Tally

After access of vehicle is allowed into a premise, card or tally should be issued to the driver, the number-of which should be written against their names and car plate number or the vehicle registration.

b)   Vehicle Register

 This is to register the number plates of visiting vehicles and the names of the drivers and the time they came and left the premises, in the vehicle register or logbook

c)   Drivers Card Access System

The drivers should be given visitors tags to hang in the front of their pockets to   help distinguish between internal staff and visitors, and they should be directed on what to do according to security policy.

2.   Staff Access Control

It must be realised that security can best be achieved when all kinds of activities are controlled and monitored, including the activities of staff in a responsible center. Not all staff of the company has access to any office or room in the company. While some have the right to access one room or office others do not have. It is then necessary to distinguish through access control measure, those who have right to access a particular place and at a particular time and those who are not. For instance, while some staff have right to access computer rooms, warehouses, stores, accounts section etc. others are not allowed to access such areas. Here, staff access control is necessary. The other aspect of staff access control is the need to identify and distinguish the difference between staff of a company and visitor. Staff can be instantly identified if their identity cards are hanged in front of their clothing. If done appropriately, staff access control is a discretionary way of controlling the access of staff, which will guarantee more security of life and property.

3.3   Quality Words for Quality Service (Procedures)

All access Points should be manned as a matter of necessity, and visitors should be thoroughly scrutinised at the guard post. Those who need assistance should be directed or referred to the reception point for further assistance. Quarreling, insults and even fighting do occur because of poor or loss of communication between the security staff and visitors. This is because most people, who are ignorant of security operations and the protective roles of security in a particular building, believe that the security staffs are hindrances or obstacles across their path. And because of this negative feeling and belief, they approach security staff in a very aggressive and uncooperative manner.

SELF-ASSESSMENT EXERCISE

Explain the acronym QWQS.

3.4   Quality Words for Quality Service (Questions for Visitors)

To avoid quarrel and misunderstanding, the security staff should use the following QWQS questions daily to question visitors before entry is allowed:

- "Welcome Sir, can I help you" (appear confident and look straight into visitor's eyes).
- "Who do you want to see, Sir?"

- "Is there any appointment" or "Is he expecting you"
- "Let me contact him" (If there is any doubt try to confirm)
- "OK, please hang this on" (Give him visitor's card if visit is genuine / approved and direct him to book down his presence in the visitor's book)
- "Do you know how to get to his office?" (Escort or direct him where necessary)
- "Our visitors' tag, Sir" (Remind visitors, and collect the tags when they are leaving)
- "Good-bye, thank you, Sir"

4.0   CONCLUSION

In this unit, you have examined in detail the term "Sample of Security Procedures for Access control at the gate. You have learnt the processes of physical Access control, and examined what the functions at the gate applies, before using quality words for quality service (QWQS).

The unit also looked at the various administrative procedures and behavioural approach beginning from the basic knowledge of security theories, and the need to know the basis of Access protection and effective control, to the behavioural School of Business and organisational security management thoughts.

5.0   SUMMARY

In this unit, we have acquired the experiences about the overview of principles and issues in physical security, Access Control Business and organisational security management.

We also examined the challenges embodied in the various aspects of security Access, such as visitors, staff and vehicles for easy operations.

6.0   TUTOR-MARKED ASSESSMENT

1. What do you understand by the term "Access control procedures"?
2. What are the three major types of Access?
3. Enumerate the functions of QWQS.

7.0   REFERENCES/FURTHER READING

Momodu, B. (2001). *The Basic of Security knowledge and Planning.* Lagos: Olucity Press Ltd.

Umar, S. (1997). *Security Operations Guard Force.* Lagos: Jo-Sekyson, K Publishers.