International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 3, May-June 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Staff Security: An Introduction

Paul A. Adekunte[1], Matthew N. O. Sadiku[2], Janet O. Sadiku[3]

[1]International Institute of Professional Security, Lagos, Nigeria
[2]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View
[3]Juliana King University, Houston, TX, USA

ABSTRACT

The security of the staff in any organization should be a priority. the provision of a safe and secure working environment is essential to the success of an organization. due to the varying levels of security risks that different organizations may be exposed to, there is urgent need to put in place security measures to protect the employees and the organization. to this end, employers must ensure the safety of their workforce by use of workplace surveillance and the compliance to the collection of personal information about existing staff and job applicants with the data protection act and the general data protection regulation (GDPR). security management would involve context analysis and risk assessment which should be followed by establishing of security procedures, contingency plans and strategies. this paper provides an insight into the issue of staff security and how to ensure safety of an organization's workforce.

KEYWORDS: *Staff security, Workplace, Security policy, Security checks*

How to cite this paper: Paul A. Adekunte | Matthew N. O. Sadiku | Janet O. Sadiku "Staff Security: An Introduction" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-3, June 2024, pp.239-244, URL: www.ijtsrd.com/papers/ijtsrd64864.pdf

IJTSRD64864

INTRODUCTION

The word “security” is from the Greek word “Se-cura” meaning “to be in a state of no fear.” Security is the protection of a person, property or organization from attack. The theory of security is to know the types of possible attacks, to be aware of the motivations for attacks and your relationship to those motives.

Staff security is basically the process to protect an employee from work related illness and injury and to make the workplace (e.g. building, etc) secure from intruders. Companies should have an environmental, safety and health policy statement, i.e. a workplace safety plan or a workplace security policy.

IMPORTANCE OF STAFF SECURITY

Since people are the heart of any business and workplace, they are invaluable assets to protect. A workplace security policy means that the employees and visitors will feel safe entering the workplace. This will be for a better workplace experience for everyone coupled with a better reputation for the business [1, 2]. The workplace security strategy is to protect the business critical data and information from hackers and other cyber security threats, and it makes you compliant with updated laws and regulations in your country or region. There is also the need to ensure that the collection of personal information about existing staff and job applicants complies with the Data Protection Act and the General Data Protection Regulation (GDPR) [3]. Security in the workplace includes both physical and digital security. Physical security refers to all of the physical assets in your workplace, such as the employees, your equipment, your visitors, and your office. Digital security refers to the protection of data, information, compliance, and systems. Some of these assets may not be seen or touched, but are vital to the success and integrity of the business.

The reasons security is of crucial priority in the workplace include the following:

- Workplace security keeps employees and visitors safe
- Workplace security protects your data and systems
- Workplace security controls access to any building
- Workplace security keeps you compliant

WHO IS RESPONSIBLE FOR SECURITY OF STAFF?

The employers are responsible for staff security, with the main responsibilities in [4]:

- Carrying out risk assessment in the workplace to determine if there are enough procedures in place to protect people.
- Identifying those who need protection from hazards, including members of staff, contractors, part-time workers, and people with specific requirements.
- Implementing safety procedures by providing and maintaining all that is needed to keep people safe, e.g. training and equipment.
- Creating a health and safety policy for all staff, including fire safety and first aid.
- Giving employees information about health and safety issues in the workplace and how they can be protected.
- Providing training to help staff understand the risks they may face in their specific roles.
- Displaying a health and safety poster, which is a legal requirement.
- Providing a first aid kit, and a number of first aiders who have received practical training.

WORKPLACE SECURITY

This has to do with policies and procedures put in place to ensure the safety and health of employees within a workplace. It involves hazard identification and control according to government standards and ongoing safety training and education for employees. To some people, workplace security means being able to hang onto a job; but for business owners, it means protecting the organization from all kinds of potential threats e.g. theft, unlawful entries, fire breakouts, kidnappings, etc. One way of safeguarding the staff is to carry out a staff risk assessment and then take action to minimize those risks. This could be by introducing monitoring technology, e.g. CCTV surveillance. Tools that can improve workplace security are [5], as shown in Figures I and 2.

- Access control technology: This can assume different forms such as badges, QR codes, facial recognition, and touch ID. With these, one can control those who enter the building and with what level of permission, ensuring that people and property are protected.
- Sensors and alarms: This could help detect security breaches, e.g. use of motion sensors can trigger an alarm if someone enters a restricted area. Smoke detectors can alert personnel to potential fires. By using sensors and alarms, one can ensure quick response to security threats and prevent damage or theft.
- Password protection tools: A password protection tool like Okta ensures that the passwords on shared company accounts are walled off behind multiple authentications.
- Visitor management system: A visitor management system (VMS) ensures that only authorized visitors are allowed into the workplace. It helps to avoid unwanted guests and security breaches.

HIGH RISK SITUATIONS FOR STAFF

There are situations where the safety and the security of staff may be at risk, which may include [6, 7]:

- Lone working
- Handling cash
- Bank runs
- Late-night working
- Getting home safely
- Business travel to certain cities or countries
- Mobile working e.g. drivers, sales representatives
- Access to commercially sensitive information
- Key holder or high level security access
- Electrical accident
- Exposure to dangerous chemicals
- Machinery and tools hazard
- Workplace harassment
- Fire accidents
- Workplace theft
- Workplace existing health conditions

After assessing the risks to the workers, next is to assign someone to implement any measures needed to reduce those risks, some of which could be:

- The installation of CCTV surveillance in appropriate locations
- Providing any appropriate training e.g. personal safety training
- Getting the latest information on the place a member of staff is planning to go on business
- Having a policy where necessary e.g. on how you may help staff get home if they finish working late at night or on what staff should do if they are physically threatened or attacked.

It should be noted the risk assessment and safety policies should be reviewed regularly.

Any employed security staff should be made to undergo suitable training. Also all staff must be given security passes and be trained to challenge unfamiliar visitors. If a member of staff becomes a victim of crime while at work, i.e. when assaulted:

- Report the incident to the police
- Record the incident
- Take steps to prevent similar incidents in the future

Staff security or security generally must be looked into holistically. Consider the following areas:

Personal movement control: Perimeter barriers are not enough security, hence the need for personnel movement control system to avoid unauthorized entry, i.e. through access list, personnel recognition, security identification cards, badge exchange procedure, and personnel escort.

Protective barrier: This is used to define the physical limits of an organization. This gives two important benefits to physical security posture i.e.

1. It creates a psychological consideration for anyone thinking of unauthorized/illegal entry.
2. Barriers have a direct impact on the number of security posts needed and on the frequency of use for each post.

Protective lighting: This affords one the degree of protection during the hours of darkness. It acts as a deterrence to thieves and vandals, and makes the work of the saboteur more difficult. Adequate lighting to an organization, building or institution not only discourages attempted unauthorized entry, but also reveals person(s) within the area.

Intrusion detective system: Importantly, all structures designed for the storage/keeping of firearms or cash should be protected with an intrusion detective system or be under Closed Circuit TV (CCTV). Alarms must be enunciated at 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.

Lock and key system: This is widely used security device in many organizations. All containers, rooms, buildings, and facilities containing vulnerable or sensitive items should be locked when not in use. Locks generally are considered delay device only and not positive bars to entry, examples are as mentioned, as shown in Figure 3:

- Key locks
- Conventional combination locks
- Manipulation resistant combination locks
- Relocking devices
- Cyber locks.

Security forces: In any organization, the security force provides the enforcement medium in the physical security program. The force consists of persons/personnel specifically organized, trained and equipped to protect the physical security interest of the organization. This is the most effective and useful tool used for comprehensive integrated physical security program.

Security control post/room: This is a prerequisite which must be integrated with intelligence in the overall strategy in planning for the defense of an organization. The security post should co-ordinate policies and procedures for organization's physical security program. It is also responsible for administering and maintaining the program, and for conducting physical security inspection such as ID cards and cars coming in and going out of the organization or company, as shown in Figure 4.

Security education: Any security system design to combat security threats cannot be effective without good security education programs. Without active interest, participation and support of every staff member in the organization, security personnel cannot effectively accomplish their mission. This can only be secured through active security education programs. The objective of security education programs include among others, to acquaint all personnel with the reasons for security measure, and to ensure their cooperation.

Loss prevention and control: Organizations and businesses must be concerned with loss prevention and control efforts as constituting part and parcel of security countermeasures. The selection of countermeasure for every risk is four, i.e.

1. Procedural controls: Policy tells us what we must do, whereas a procedure tells us how we are going to do it.

2. Hardware (fences, gates, locks, keys, barricades, etc.): This is the use of padlock, lockable suitcases, chains and locks to protect bicycles, motorcycles, front door peepholes, night latches, outdoor lighting, safes, lockage file cabinets, and vaults.

3. Electronic systems: Automated access control systems, alarms, CCTV, intrusion alarms, motion detection alarms, sound or vibration alarms, smoke alarms/detectors, heat detectors, etc. Electronic alarms have proved to be more reliable than people for a number of reasons, i.e. they are: i. Less costly compared to annual salaries of personnel, ii. They do not fall asleep, iii. They are always on the job, and iv. They are honest.

4. Personnel: The rule of the thumb is to use people only in those areas where procedural controls, hardware or electronics cannot be employed more efficiently. Obviously, there are security functions for which people are the best and sometimes the only countermeasure e.g. where ability to exercise judgment is needed, overseeing employees as they leave work in a production plant, guard post and patrols, inspection, investigations, prevention of criminal attacks, maintaining order, crowd control, etc.

It is the aspect of security operation which constantly breads contempt, resentment, antagonism and conflict in any responsibility centre. 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 business today, it is very unfortunate to observe that many organizations 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, quarrelling, conspiracy and lawlessness will become the order of the day around such organizations, between security operatives 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. The three types of security policies in common use are:

1. Program policies
2. Issue-specific policies
3. System-specific policies.

By definition, security policy refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information included in it. A good policy protects not only information and systems, but also individual employees and the organization as a whole. In the security policy, the 5 key elements too must be present as per the US Department of Defense promulgated Five Pillars of Information Assurance (IA) model which includes the protection of:

- Confidentiality
- Integrity
- Availability
- Authenticity and
- Non-repudiation of user data. [8]

A company's security policy must also include policy formulation, policy on security, policy on recruitment, policy on employee dishonesty and crimes, policy on retrenchment, policy on searching, and policy implementation.

Organizations are strongly advised to conduct background checks and verify applications of all potential employees and contractors. This is to help expose any undesirable or unqualified candidates, such that a dishonest applicant should not be given the opportunity to become a dishonest employee. The basic background checks and verification may include the following information:

- Criminal records
- Citizenship
- Employment history
- Education
- Certifications and licenses
- Reference checks (personal and professional)
- Union and association membership
- Credit records
- Drug testing

CONCLUSION

Staff security importance cannot be overemphasized as it protects the people, information and assets by enabling the organization to reduce the risk of harm to people; customers and partners, reduce the risk of your information or assets being lost, damaged, or compromised; have greater trust in people who access your official or important information and assets; deliver services and operate more effectively. Personnel security focuses also on reducing the risks associated with insider threats. Hence, adequate attention and budget must be given to staff security, as well as all members of staff, without exception must be security conscious, as prevention is less costly.

REFERENCES

[1] "The importance of security in the workplace I Envoy," https://envoy.com/importance-of-security-in-the-workplace

[2] Ron Kurtus, Theory of Security, https://www.school-for-champions.com/theory-of-security

[3] Staff security and monitoring employees, https://www.nibusinessinfo.co.uk/staff-security-and-monitoring-employees

[4] Who is responsible for workplace health and safety? https://www.britsafe.org/who-is-responsible-for-workplace-health-and-safety

[5] Amy Kirkham, "The importance of workplace security: what it is and why you need it," July 25, 2023, https://envoy.com/importance-of-security-in-the-workplace

[6] "Staff security and monitoring employees," https://www.nibusinessinfo.co.uk/staff-security-and-monitoring-employees

[7] Busayo Longe, "Workplace safety and hazards: Types, Examples and Preventive Tips," https://www.formpl.us/workplace-safety-and-hazards

[8] Infinit-O, “The 5 Pillars of Information Security and how to Manage them,” April 9, 2018, https://resourcecenter.infinit-o.com/pillars-of-information-security-and-how-to-manage-them

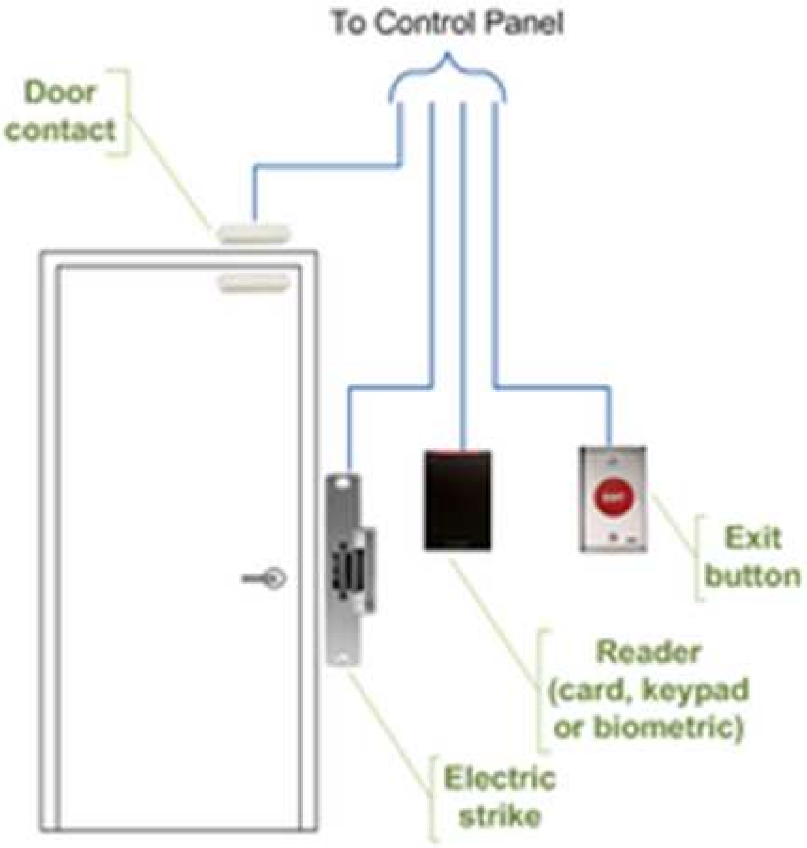

Figure 1. Access control.
https://www.google.com/search?q=access+control%3B&sca_esv=579784056&tbm=isch&sxsrf=AM9HkKl GbEhBsLfQz6rxYJG_EQXbyihtSg:1699269872005&source=lnms&sa=X&ved=2ahUKEwiws-TIoa-CAxWlV0EAHdjSBNsQ_AUoAXoECAQQAw&biw=1366&bih=580&dpr=1#imgrc=TaAu8X9t7NTx6M

Figure 2. Closed circuit television.
Source: https://en.wikipedia.org/wiki/Cosed-circuit_television

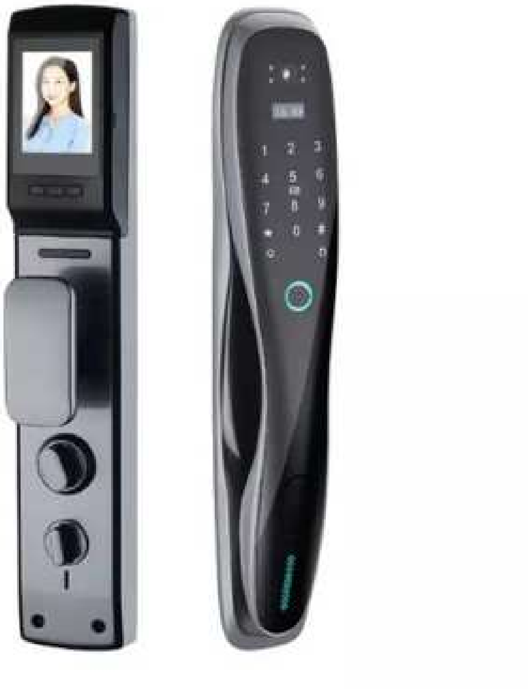

Figure 3. Cyber lock.

Source: https://www.konga.com/product/smart-lock-automatic-biometric-lock-5769348?gad_sou

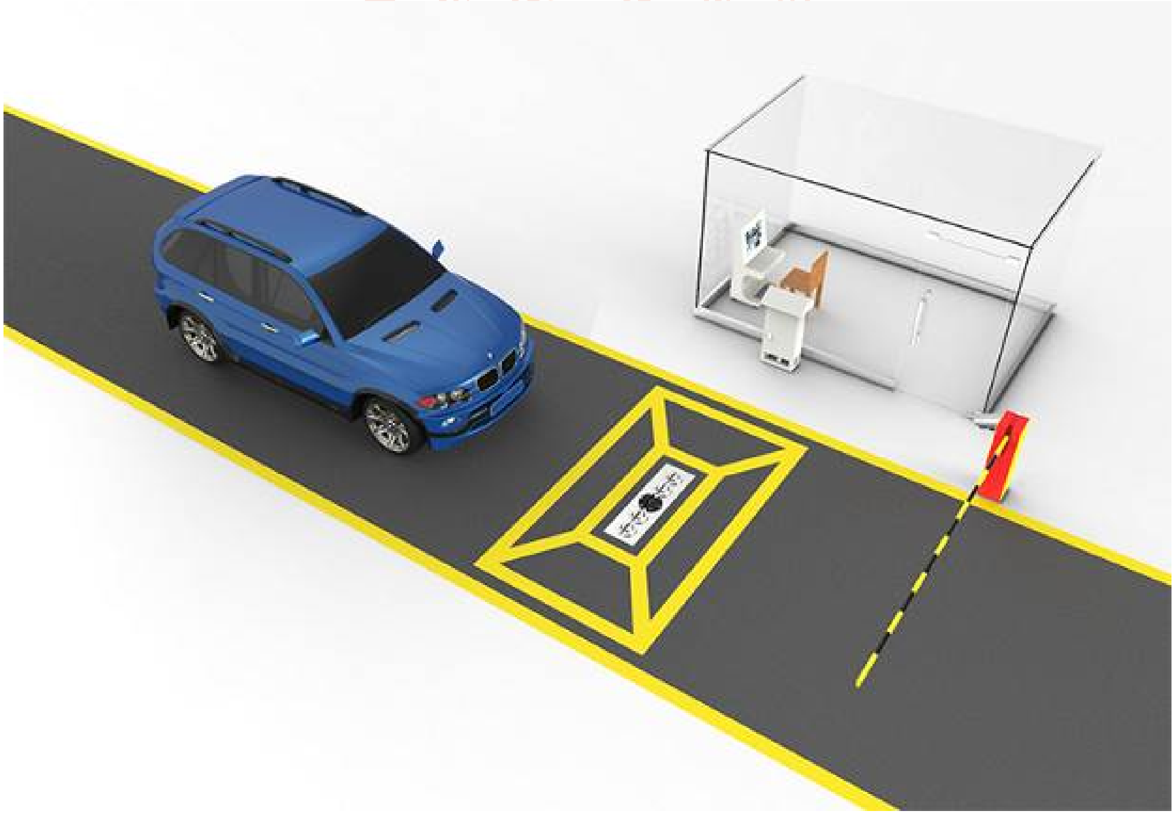

Figure 4. Under vehicle surveillance.

Source: https://www.gsautomatic.com/permanent-under-vehicle-surveillance-system-gs3300/?gclid=Cj0KCQiAuqKqBhDx...