ISRG Journal of Arts, Humanities and Social Sciences (ISRGJAHSS)

ISRG PUBLISHERS
Abbreviated Key Title: ISRG J Arts Humanit Soc Sci
ISSN: 2583-7672 (Online)
Journal homepage: https://isrgpublishers.com/isrgjahss
Volume – II Issue-V (September-October) 2024
Frequency: Bimonthly

Insider-Crimes and Security Management of Business Organizations

Akankpo, Udom E.

Department of Sociology University of Port Harcourt

| **Received:** 06.09.2024 | **Accepted:** 11.09.2024 | **Published:** 12.09.2024

***Corresponding author:** Akankpo, Udom E.
Department of Sociology University of Port Harcourt

Abstract

All business organizations in all countries and at all times suffer insider-crimes in general. The insider criminal accounts are difficult to detect because most are planned in details, some take advantage of existing security laxes and others due to opportunity. Crime Opportunity Theory (COT) is the crux of the study. A criminal is attracted to an object of value when there are no persons or equipment to guard it. An insider crime is a motivation of indication of failure on the part of management to adequately engage security at the business place. Expositive method was adopted for the study, with the aim as a review and compilation of security measures at reducing/preventing crimes in business organizations. The study proves that, an insider crime exists at every level of the business organization, from management to junior workers, from production, distribution chain and marketing sub-units. The means to insider crime is opportunity of free access to business premises, information, persons. It is recommended that, since insider security is relative to the business organization, products and services, management factors and polices, environment, number of employees and management styles, effective communication, team building, reporting system and punishment will help reduce operations.

Keywords: *Insider, Crimes, Business organization, Security*

Introduction

All business organizations in all countries and at all times suffer insider-crimes in general. This tend to confirm the industrial security 10-10-80 rule that, 10% of workers never steal, 10 % of workers will steal whenever the opportunity present itself, while the remaining 80% will be motivated to steal or not to. Insider crime occurs when there are vulnerabilities, risks are low, employees are not motivated (personal financial needs) and opportunities are available. The U.S. Department of Justice noted that, the criminal that is difficult to discover and who must have caused so much frustrations to business is the insider – the member of staff with guaranteed access. The economic productivity and security management of businesses in a continuous pace devoid of liquidation are factors of a successful business. Uncertainty on the other hand, changes business functioning and environment. However, businesses are expected to experience both declining and growing rates sometimes from market factors, but when the economic phenomenon is a security breach from a member of staff, much has to be feared. This is because security components

DOI: 10.5281/zenodo.13752852

(guards and electronics) are limited to some security measures and control to what an insider can undertake.

Today, business organizations are faced with many challenges, such as declining sales, pandemic, harsh government policies, theft and including insider crimes. Smokvina and Yankovska (2019) observed that, members of staff are either a root of crimes or a personnel security target. These crimes range from fraud, stealing, damage, violence etc. But yet, improving competitiveness of the business is measured by the competency of personnel who are granted access and trust to function. The challenges facing most businesses today is protection against threats related to the operations of the organization. These threats are opposed to the goals, profits and progress of the business. The highest of the treats had been the insider-crime, which raises the question of – how can an organization overcome human crime by the employees? Hence, crime prevention is a major concern for business owners, as losses greatly affect production and profitability.

This study therefore is a review and compilation of security measures at reducing/preventing crimes in business organizations. To make many businesses less vulnerable to insider-crimes, the purpose of the study is to fill in the void in literature on the role of insider-crimes; to offer employee modes, and to propose management principles to adopt in minimizing them. And the expositive method is adopted for the write up.

An Overview of Insider Tactics

A business organization is an entity that is formed for the essence of operating a commercial enterprise, with the resources of persons and materials to achieve a common goal. To succeed, security management is necessary in harnessing all aspects of the organization's assets (people, buildings, finances and products) against risk. An insider is a person with authorized access to a business organization by virtue of an employment. According to Cybersecurity Agency (2020) 'an insider is any person who has or had authorized access to or knowledge of an organization's resources (finances), including personnel, facilities, information, equipment, networks, and systems" p.9. Insider crime therefore is any act against the law in which an employee uses the authorization clause to cause either physical, personal or financial wrong against the smooth running of the business.

An insider crime varies. Some crimes are however unintentional (neglect, accident), while some are intentional (stealing etc.). The insider criminal accounts are difficult to detect because most are detailed planned, some take advantage of existing security lax and others due to opportunity. All these take place because of the pattern of operations. Three types of insider-crime modus have been identified by Hoffman, Meyer, Schwarz and Duncan (1990) as:

1. Insider alone – either creating lone opportunities or utilizing the existing ones.
2. Insider(s)/Outsider(s) - conspiring with outsider(s) of the business organization.
3. Insider(s)/Insider(s) – conspiring with peer(s) within or outside the unit of the organization.

When an insider offender is caught, Hoffman et al. (ibid) enumerated steps into the investigations. Such as identification of the employee, years of service in the organization, age, status, gender and modus (procedures). The motivating factor(s) are necessary as well as the nature of crime committed. Another avenue to consider is the lapses or effectiveness of the security procedures leading to the crime. Also, of importance is the prevention model to reduce or prevent reoccurrence.

Literature Review

A number of studies have been initiated to uncover the reasons behind employee theft or crime in general. Such include the works of Korgaonkar, Becerra, Mangleburg and Bilgihan (2021) that crimes of individuals working in business organizations bring such actions as tax loss and loss of revenue. They equally noted that employee's idea of security systems within the organization offer the insider no arrest or pursuit. Kennedy (2017) observed several negative impacts on employers, employees and stakeholders. According to the analysis of the National Retail Federation (2018), shoplifting recorded 35.7%, employee theft stands at 33.2%, administrative omission is 18.8%, unknown sources is 6.6% and vendor fraud is 5.8%.

In the construction industry, Ablordeppey, Moo, Akorsu and Mustapha (2020) explained that insider-crime exists because the contractors and employees all understands the work place environment along with the security processes. Iwuagwu (2014) posit that there is an interrelationship with business locations in central business districts and idleness of workers with crime rate.

Under environmental factors, Warne (2016) noted that crime at business places increase in or around high commercial places and cities. Edike and Babatunde (2017) highlighted the underutilization of security apparatus and systems, such as CCTV, alarms and profiling of applicants in reducing incidents.

Crime Opportunity Theory (COT) is the crux of the study, though a subset of Routine Activity Theory (RAT). It was developed by Cohen and Felson (1979) and states that, crime happen as a motivated offender (criminal) is attracted to a target (an object of value) when there is no capable guardian (security guard or equipment). Hence, crime according to the theory is a product of three elements: 1. A criminal, 2. Object of value and 3. Absence of a guard/systems.

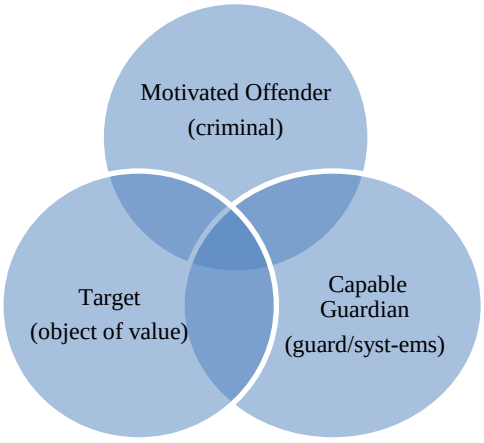

Figure 1. Criminal behaviour connectivity

The theory explains the connectivity of behaviour that exist when a crime is about to occur, stating that, there is a routine order or process in that, a criminal is attracted to an object of value when there are no persons or equipment to guard it. Hence, there is crime within the time-frame of the absence of guard. This implies that, an insider-crime is a motivation of an indication of failure on the part of management to adequately engage security at the business place, or on objects of sales, or on their persons, leading to breakdown of business activities.

DOI: 10.5281/zenodo.13752852

Major Sources of Losses

Smokvina and Yankovska (2019) noted that, members of staff are major source of crime in the destruction of information, stealing of funds and materials of business organizations. It implies that an insider alone or in interaction with the external body, with the influence of internal mechanism, in separate time periods may cause crimes in his/her business organization.

Some employees are full of dysfunctional behaviours that are detrimental to the economic development of the business organizations that they work. Some of these behaviours are sometimes economic and non-economic. The direct economic crimes are stealing, fraud, damage, diversion, robbery, unofficial but private practices, faking of products, influencing supplies. Staff approaches to organizational incidents and crimes include false audit, poor record keeping, monitoring/tracking of communication and other business processes, delay in timely execution of job schedule, refusal to complete some vital forms, intentional omission, dilution, delivery of incomplete goods, acceptance of bribe, breaking and entry, faking of product, pilfering, vandalism, issuance of illegal receipt, use of private Point-of-Service machine, kidnapping of principal members of staff, serving the interest of another organization, threats, concealment of goods, removing centre loads/goods, re-wrapping, rearranging top layers, false delivery, damaged goods fraud, breach of modes of operation, murder, malfeasance, decline in competitiveness, spreading negative information, minimizing business reputation of both employee and organization. The non-economic crimes include violence, drugs/substances abuse and lonely/isolated behaviours.

Strengthening Employee Value

How can employees minimise theft in the workplace? Bunn and Glynn (2013) had identified background screening, accounting details and monitoring of staff to confirm trustworthiness. Other issues for consideration are motivation of morale and provision of incentives to actively participate in achieving organizational goals.

Korgaonkar, et al. (2021) wrote that, social and situational elements as well as moral values also help as an index to employee theft as a result of organizational vulnerability. Studies by Brooks and Writer (2013); Cox, Cox, and Moschis (1990) all inform that, stealing is a cause of office environment and the level of mental/moral growth. Criminal behaviours are generally rooted in many factors, especially social, which involves peer influence and social class attainment.

Analysis of Security Process

An insider crime exists at every level of the business organization, from management to junior workers, from production, distribution chain and marketing sub-units. Other departments involved are procurement, store, security, including finance and administration. Approach to insider-crimes can be classified into three, namely; (a). personnel (b). property and (c). product or services.

Insider-crime(s) are targeted at some persons in the business organizations for various reasons. Some as vengeance to the management due to policies and targeted at the structures. The last is aimed at the products or services of the business. The approaches are either alone in committing any crime. The second group is an insider(s) in connivance with another insider(s). The third category is insider(s) with outsider(s) who may be visitors, contractors, service agents, former employees, sales representatives, drivers, friends, family members and competing organization(s).

Table 1. Analysis of Insider-Crimes Processes

Crime Modes	Targets	Pursuits
Insider **Insiders** **Insider(s)/Outsider(s)**	**Personnel**	Assaults, murder, kidnap, substances abuse, irregularities, poor performance.
	Property	Arson, stealing, breaking & entry, damage, disruption of services.
	Products/Services	Finance, information, trade secrets, documents, economic espionage.

Enhancing the System

The means to insider-crime is **opportunity**. Free access in to business premises, information and persons. Therefore, every internal and external mechanisms to curtail continuous crimes lies on minimising opportunities. There must be multiple approaches to be adopted to forestall continuous acts. The recommended classifications are hereunder enumerated:

1. **Physical security** – Security guards, spontaneous audit, extra protection of access to critical property/knowledge, security awareness training, monitoring of workers at rush hours, investigations of minor complaints/suspicions, recruitment control, mandatory documentation of all business transactions, personnel protection, regular changing of keys/padlocks, reinforcing entrances/perimeters, enforce badge permit at critical areas, tracker alarm, time-delayed safe, develop security policies, reduce cash movement, spot checks and security mirrors.
2. **Cybersecurity** – Restrictions of access to critical units, password protection, enhanced rules of usage/access, dead drop, install anti malware, bolster data and computer fire walls.
3. **Surveillance** – Close-circuit television, remote accesses, evaluation of work output, monitoring movement of information/documents/materials/deviant behaviours, adopt hidden cameras, practicing a two-person team, monitor shift duty, monitor activities in and out of facility.

Conclusion

Events and experience has shown that, total security cannot be attained, and insider-crimes completely eliminated. This is because insider security is relative to the business organization, products and services, management factors and polices, environment, number of employees and management styles. Effective communication of anti-crimes within the organization helps reduce criminal activity. Team building in the workplace serves to monitor one another. Reward on reporting system as well as punishment award may withdraw motivation. Engage business stakeholders as watchdogs, including high disciplinary measures as well as severe legal sanctions.

DOI: 10.5281/zenodo.13752852

References

1. Ablordeppey, E. E., Moo, F., Akorsu, W. & Mustapha, A. (2021). Minimising theft on construction sites in Ghana: The perspective of contractors in the Upper West Region of Ghana. Civil and Engineering Research, 12(5), 30-40.
2. Brooks, C. & Writer, B. S. (2013). Employee theft on the rise are expected to get worse. Business News Daily.
3. Bunn, M. & Glynn, K. (2013). Preventing insider theft: Lessons from the casino and pharmaceutical industries. Journal of Nuclear Materials Management, 41(3), 4-16.
4. Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(40), 588-608.
5. Cox, D., Cox, A. D. & Moschis, G. P. (1990). When consumer behaviour goes bad: An investigation of adolescent shoplifting. Journal of Consumer Research, 17(2), 149-159.
6. Edike, U. E. & Babatunde, A. (2017). Crime prevention on construction site: A study of Ogun State, Nigeria. Covenant Journal of Research in the Built Environment, 5(1), 32-47.
7. Hoffman, B., Meyer, C., Schwarz, B. & Duncan, J. (1990). Insider crime: The threat to nuclear facilities and programs. U.S. Department of Energy, RAND.
8. Iwuagwu, C. (2014). Statistical appraisal of crime rate in Nigeria. Journal of Physical Science and Innovation, 6(1), 38-48.
9. Kennedy, J. P. (2017). Functional redundancy as a response to employee theft within small businesses. Security Journal, 30(1), 162-183.
10. Korgaonkar, P., Becerra, EP., Mangleburg, T. & Bilgihan, A. (2021). Retail employee theft: When retail security alone is not enough. Psychology & Marketing, 1-14. https: doi.org/10.1002/mar.21460.
11. National Retail Federation (2018). SO18 National retail security survey. Retrieved from https:///cdn.nrf.com/sites/default/files/2018-10/NRF-NRSS-Industry-Research-Survey-2018.pdf
12. Smokvina, G. & Yankovska, O. (2019). Personnel security of the industrial enterprise: Its essence, constituents and measures of minimization of threats. Economic Journal Odessa Polytechnic University, 1(7), 38-45.
13. Warne, L. (2016). Crime in the construction industry. Retrieved from https://prime-secure.co.uk/wpcontent/uploads/2021/02/CIOB-Crime-in-the-Construction-Industry.pdf on 10-10-2023
14. Insider threat mitigation guide (2020). Cybersecurity and Infrastructure Security Agency. Retrieved from https://umbrella.cisco.com on 12-10-2023

DOI: 10.5281/zenodo.13752852