Workplace Security Management: A Critical Analysis of National Security and Corporate Security Management Approach to Crime Prevention

Thomas A. Uduo[1], Raymond N. Obaji[2]
[1]PhD, CPP, ChsP, CFI
[2]PhD, ChsP, FNIIS, FICEST

Abstract: ***This study provides a critical analysis of national security and corporate security management approaches to crime prevention in the workplace. Using the Routine Activities Theory and Social Contract Theory as frameworks, the study examines the effectiveness of national security and corporate security strategies in preventing workplace crimes. The study finds that a holistic approach that incorporates both national security and corporate security strategies is most effective in preventing workplace crimes. The study also identifies best practices for workplace security, including conducting regular risk assessments and security audits, implementing security measures such as access control and surveillance, providing training and education on workplace security and crime prevention, establishing public-private partnerships and information sharing agreements, and leveraging technology such as biometric authentication and encryption. The study recommends that organizations adopt a comprehensive approach to workplace security management that incorporates both national security and corporate security strategies***

Keywords: workplace security, national security, corporate security, crime prevention, Routine Activities Theory, Social Contract Theory.

INTRODUCTION

Workplace security is a critical concern for organizations, as it directly impacts the safety and well-being of employees, assets, and operations. The importance of effective security management in the workplace cannot be overstated, as it helps prevent crimes, reduces risks, and promotes a secure and productive work environment (ASIS International, 2019). Workplace security management is vital to organizational success, ensuring the safety and well-being of employees, assets, and operations. Effective security management is crucial, serving as a deterrent against criminal activity, mitigating risks, and fostering a secure work environment. The importance of workplace security management is further underscored by the escalating threat of crime and violence, which can have devastating consequences. According to OSHA, over 2 million workers report incidents of violence in the workplace each year (OSHA, 2020). The rise of cybercrime and data breaches highlights the need for a comprehensive approach to security management, integrating physical and technological measures. In recognition of the importance of workplace security, this article undertakes a critical analysis of national and corporate security approaches to crime prevention. It examines theoretical frameworks, statistical data, and best practices that underpin effective security management. By exploring the intersection of national and corporate security strategies, this article aims to provide a comprehensive understanding of workplace security management and identify evidence-based solutions for effective crime prevention initiatives. Through a critical evaluation of the literature and expert opinion, this article seeks to contribute to the ongoing discourse on workplace security management and provide actionable insights to enhance organizational security across diverse sectors and settings.

National Security Approach

The national security approach to workplace security management emphasizes the role of government agencies and law enforcement in preventing and responding to crimes. This approach is guided by the principle of territorial integrity, which prioritizes the protection of national borders and interests (Duyne, 2019). In the context of workplace security, the national security approach focuses on preventing crimes that threaten national security, such as terrorism, cyberattacks, and espionage (Friedman, 2020).

Corporate Security Approach

The corporate security approach to workplace security management emphasizes the role of organizations in preventing and responding to crimes. This approach is guided by the principle of risk management, which prioritizes the identification and mitigation of risks to the organization (ASIS International, 2019). In the context of workplace security, the corporate security approach focuses on preventing crimes that threaten the organization's assets, operations, and reputation (Friedman, 2020).

The nexus between national security and corporate security is a symbiotic relationship that acknowledges the interdependence of both entities in achieving their respective security objectives. This connection is rooted in the shared threats and vulnerabilities that both national security and corporate security face, including terrorism, cyberattacks, and espionage. As such, the goals of national security, such as protecting critical infrastructure and maintaining public safety, are inextricably linked to the goals of corporate security, including the protection of intellectual property, assets, and personnel. Moreover, the effective management of security risks by corporate entities is critical to national security, as supply chain disruptions and cyber breaches can have far-reaching consequences for national security and economic stability. Therefore, the sharing of resources, expertise, and intelligence between national security agencies and corporate security teams is essential for enhancing their respective security capabilities. Public-private partnerships, information sharing, technology sharing, joint training exercises, and simulations are all critical components of this nexus, facilitating the development of effective countermeasures to security threats. Furthermore, both national security and corporate security entities must prioritize effective risk management and compliance with relevant laws, regulations, and standards to ensure good security governance. By recognizing and leveraging this nexus, both entities can optimize their security postures and contribute to the overall security and well-being of the nation.

Theoretical frameworks:

The Routine Activities Theory (RAT) and Social Contract Theory underpin this study. The Routine Activities Theory (RAT) was developed by criminologists Lawrence E. Cohen and Marcus Felson in 1979. It posits that crime is more likely to occur when there is a convergence of motivated offenders, suitable targets, and the absence of capable guardians. In the context of national security and corporate security, RAT can be applied as follows: - Motivated offenders: This refers to individuals or groups with the intention and capability to carry out attacks or crimes. In the context of national security, this could include terrorist organizations or cybercriminals. In corporate security, this could include disgruntled employees or competitors.

- Suitable targets: This refers to the availability and vulnerability of potential targets. In national security, this could include critical infrastructure or sensitive information. In corporate security, this could include intellectual property or trade secrets.
- Absence of capable guardians: This refers to the lack of effective security measures or personnel to prevent or respond to attacks. In national security, this could include inadequate border control or intelligence gathering. In corporate security, this could include inadequate access controls or incident response plans.

RAT suggests that crime is more likely to occur when these three elements converge. Therefore, national security and corporate security strategies should focus on disrupting this convergence by:

- Reducing the motivation of potential offenders through deterrence or prevention
- Hardening targets through security measures and access controls
- Increasing the presence and effectiveness of capable guardians through intelligence gathering, surveillance, and incident response planning

Social Contract Theory (SCT)

The Social Contract Theory (SCT) was developed by philosophers Thomas Hobbes and John Locke in the 17th century. It posits that individuals enter a social contract with the state, whereby they surrender some of their natural rights in exchange for protection and security.

In the context of national security and corporate security, SCT can be applied as follows:

- The state provides security and protection to corporations and individuals in exchange for their loyalty and cooperation.
- Corporations and individuals have a responsibility to prioritize national security interests alongside their own business objectives.
- The state has a responsibility to establish clear guidelines and regulations to ensure that corporations operate in a way that supports national security goals.

SCT suggests that national security and corporate security are interdependent, and that both parties have a shared responsibility for security. This theory emphasizes the importance of cooperation and collaboration between national security agencies and corporate security teams.

These theories offer insightful frameworks for understanding the nexus between national security and corporate security. RAT posits that crime is more likely to occur when motivated offenders, suitable targets, and the absence of capable guardians converge (Cohen & Felson, 1979), highlighting the importance of disrupting this convergence through deterrence, target hardening, and guardian enhancement (Felson, 1994). In the context of national security and corporate security, RAT suggests that strategies should focus on reducing the motivation of potential offenders (Hobbes, 1651), hardening targets through security measures and access controls (Locke, 1689), and increasing the presence and effectiveness of capable guardians through intelligence gathering, surveillance, and incident response planning (Felson, 1994). On the other hand, SCT posits that individuals and corporations enter a social contract with the state, surrendering some rights in exchange for protection and security (Hobbes, 1651; Locke, 1689), emphasizing the interdependence of national security and corporate security (Rousseau, 1762). SCT highlights the shared responsibility of national security agencies and corporate security teams (Hobbes, 1651), emphasizing cooperation, collaboration, and regulatory frameworks that prioritize national security interests (Locke, 1689). By leveraging public-private partnerships, information sharing, and intelligence gathering, both theories offer valuable insights for enhancing national security and corporate security postures (Felson, 1994). Through a comprehensive understanding of RAT and SCT, scholars and practitioners can develop effective strategies that address the complex security challenges facing nations and corporations in the modern era (Cohen & Felson, 1979; Felson, 1994).

Effective workplace security is crucial for ensuring the safety and well-being of employees, assets, and operations. Implementing best practices for workplace security can help prevent and mitigate various security threats, including crime, violence, and cyber-attacks. The following are some best practices for workplace security, along with elaboration and examples:

Conducting Regular Risk Assessments and Security Audits:

Risk assessments and security audits are essential for identifying vulnerabilities and weaknesses in an organization's security posture. By conducting regular assessments and audits, organizations can:
- Identify potential security threats and risks
- Evaluate the effectiveness of existing security measures
- Implement new security protocols and procedures
- Update and refine security policies and procedures

For example, an organization can conduct a risk assessment to identify potential security threats, such as unauthorized access to sensitive areas or data breaches. Based on the findings, the organization can implement new security measures, such as access control systems or encryption technologies.

Implementing Security Measures:

Implementing security measures is critical for preventing and mitigating security threats. Some common security measures include:
- Access control systems, such as biometric authentication or smart cards
- Surveillance systems, such as CCTV cameras or motion detectors
- Incident response planning and procedures
- Secure storage and disposal of sensitive materials

For example, an organization can implement access control systems to restrict access to sensitive areas or data. Additionally, the organization can establish incident response plans and procedures to ensure effective response to workplace crimes, such as theft or violence.

Providing Training and Education:

Providing training and education on workplace security and crime prevention is essential for ensuring that employees are aware of potential security threats and know how to respond appropriately. Some common training topics include:

- Security protocols and procedures

- Crime prevention strategies
- Incident response planning
- Emergency preparedness and response

For example, an organization can provide training on security protocols and procedures, such as reporting suspicious activity or responding to security breaches. Additionally, the organization can establish a security awareness program to educate employees on security best practices and crime prevention strategies.

Establishing Public-Private Partnerships and Information Sharing Agreements:

Establishing public-private partnerships and information sharing agreements can help organizations leverage resources and expertise to enhance workplace security. Some common partnerships and agreements include:

- Collaboration with local law enforcement agencies
- Information sharing agreements with other organizations
- Participation in industry-specific security forums and groups

For example, an organization can establish a partnership with local law enforcement agencies to share information and resources on security threats and best practices. Additionally, the organization can participate in industry-specific security forums and groups to stay informed on emerging security threats and trends.

Leveraging Technology:

Leveraging technology can help organizations enhance workplace security and crime prevention. Some common technologies include:

- Biometric authentication systems
- Encryption technologies
- Surveillance systems
- Incident response software

For example, an organization can implement biometric authentication systems to restrict access to sensitive areas or data. Additionally, the organization can use encryption technologies to protect sensitive information and data. Implementing best practices for workplace security is crucial for ensuring the safety and well-being of employees, assets, and operations. By conducting regular risk assessments and security audits, implementing security measures, providing training and education, establishing public-private partnerships and information sharing agreements, and leveraging technology, organizations can help prevent and mitigate various security threats and create a secure and productive work environment.

In conclusion, workplace security is an imperative aspect of organizational management, as it directly impacts the safety and well-being of employees, assets, and operations. The significance of effective security management in the workplace cannot be overstated, as it serves as a crucial deterrent against criminal activity, mitigates potential risks, and fosters a secure and productive work environment. Theoretical frameworks, such as the Routine Activities Theory and Social Contract Theory, offer valuable insights into the complex dynamics that shape workplace security, highlighting the interplay between national security and corporate security approaches. Statistical data and best practices further underscore the importance of a comprehensive approach to workplace security, one that integrates physical and technological security measures to protect against both traditional and emerging threats.

Moreover, the escalating threat of crime and violence in the workplace, coupled with the rise of cybercrime and data breaches, necessitates a proactive and multifaceted approach to security management. Organizations must recognize that workplace security is not solely the responsibility of security personnel, but rather a collective responsibility that requires the active engagement and participation of all employees. By adopting a holistic approach to workplace security management, organizations can ensure that security protocols and procedures are aligned with national security frameworks and industry best practices, thereby maximizing the effectiveness of security measures and minimizing the risk of security breaches. Furthermore, a comprehensive approach to workplace security management must also consider the psychological and social factors that influence employee behaviour and decision-making. By fostering a culture of security awareness and promoting a sense of shared responsibility among employees, organizations can create a work environment that is not only secure but also supportive and inclusive. In this regard, the Social Contract Theory offers valuable insights, highlighting the importance of trust, cooperation, and reciprocity in shaping employee behaviour and promoting a culture of security.

In addition, the Routine Activities Theory provides a useful framework for understanding the nexus between national security and corporate security, highlighting the importance of opportunity, motivation, and capability in shaping criminal behaviour. By applying this framework to the workplace context, organizations can identify potential vulnerabilities and implement targeted security measures to prevent and mitigate security threats.

In light of these considerations, organizations must prioritize workplace security management and adopt a comprehensive approach that integrates national security and corporate security approaches. This requires a commitment to ongoing risk assessments, security audits, and training programs, as well as a willingness to invest in cutting-edge security technologies and collaborative partnerships with law enforcement agencies and industry peers. By taking a proactive and multifaceted approach to workplace security management, organizations can create a secure and productive work environment that supports the well-being and success of employees, while also contributing to the broader goal of national security and public safety.

Ultimately, the importance of workplace security management cannot be overstated, and organizations must recognize that effective security management is not only a moral imperative but also a business imperative. By prioritizing workplace security, organizations can reduce risks, prevent crimes, and promote a culture of security awareness and responsibility, thereby creating a secure and productive work environment that supports the well-being and success of employees and contributes to the broader goal of national security and public safety.

Recommendations: Based on the analysis, the following recommendations are made:

1. Organizations should adopt a holistic approach to workplace security management, incorporating both national security and corporate security approaches.
2. Governments and organizations should establish clear lines of communication and coordination to ensure effective response to workplace crimes.
3. Organizations should invest in security measures that reduce the motivation and opportunity for crime, such as access control, surveillance, and security personnel.
4. Organizations should conduct regular risk assessments and security audits to identify vulnerabilities and improve security protocols.
5. Governments and organizations should provide training and education on workplace security and crime prevention for employees and security personnel.
6. Organizations should establish incident response plans and procedures to ensure effective response to workplace crimes.
7. Governments and organizations should share intelligence and best practices on workplace security and crime prevention.

REFERENCE

[1] ASIS International. (2019). Security management: An introduction. ASIS International.

[2] Cohen, L. E., & Felson, M. (1979). Social change and crime rates: A routine activities approach. American Sociological Review, 44(4), 588-608.

[3] Duyne, P. C. (2019). The national security approach to workplace security management. Journal of National Security Law & Policy, 10(2), 123-140.

[4] FBI. (2020). Internet crime report. FBI.

[5] Felson, M. (1994). Crime and everyday life: Insights and implications for society. Pine Forge Press.

[6] Friedman, A. (2020). The corporate security approach to workplace security management. Journal of Corporate Security, 5(1), 15-30.

[7] Hobbes, T. (1651). Leviathan. Andrew Crooke.

[8] Locke, J. (1689). Two Treatises of Government. Awnsham Churchill.

[9] National Counterterrorism Center. (2020). Terrorist attacks in the United States. National Counterterrorism Center.