International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Awareness and Practices of Security Management Agency Deployed in Asia Brewery, Inc.: Basis for Action Plan

Aldrin C. Danao

University of Cabuyao
Philippines
Aldrindanao77@Gmail.Com

ABSTRACT

Security management awareness and implementation are essential components of a comprehensive organizational risk mitigation framework. In a rapidly evolving threat landscape, the role of security personnel in adhering to standardized procedures is vital for ensuring the continuity and safety of business operations. This study focused on evaluating the awareness and practices of the security management agency assigned to Asia Brewery, Inc., with the intent of establishing a solid foundation for a tailored action plan aimed at improving overall security performance.

Through a qualitative research design, the study utilized validated survey instruments to collect data from security personnel regarding their familiarity with existing security protocols, adherence to procedures, and perception of workplace threats. A licensed statistician processed and analyzed the results to identify patterns, lapses, and strengths within the current security framework. The findings revealed a mix of strong foundational knowledge in some areas and notable deficiencies in others, particularly regarding the consistent implementation of policies and situational response readiness.

Based on these insights, the study proposes an action plan emphasizing continuous training, improved policy dissemination, and regular security audits. The ultimate goal is to foster a culture of accountability and preparedness among security staff, thereby enhancing the safety and resilience of the workplace.

Key words: Security Awareness, Security Management Practices, Workplace Safety, Organizational Security, Risk Mitigation

1. INTRODUCTION

In today's fast-paced and ever-evolving business landscape, security management has become a cornerstone for safeguarding assets, maintaining operations, and ensuring the resilience of an organization. Stakes are higher than ever at Asia Brewery, Inc., a leading player in the beverage industry.

As the company continues to expand its footprint, the complexity of potential security threats escalates, demanding a robust and proactive approach to security management.

According to Tulane University (2023), in Louisiana, United States, security management is the duty and activities necessary for overseeing the security environment, including security measures and policies. It includes the availability, confidentiality, and integrity of service. It is therefore the responsibility of a security manager to make sure that all security procedures are followed to protect the physical assets and data of an organization from known as well as current threats. Additionally, security managers are responsible for managing and training the company's internal security personnel, which consists of anything from network security specialists to facility guards. Enforcing the organization's security standards and procedures concerning all personnel, including alerting them to new security guidelines and preparing them to recognize and address threats, will also fall within the security manager's purview.

The face of security management has evolved since the early 1900s. Managers today need to constantly adapt if they want to keep ahead of the myriad potential threats. Without question, security management is a strategic competency that gives companies the ability to spot possibilities and gain a competitive advantage (Zammani et.al., 2021). Conversely, such variation can be attributed to differences in resources, training, and regulatory frameworks. In a global survey conducted by the International Association for Security Management (IASM), it was found that awareness of physical and cybersecurity threats has increased significantly over the past decade. However, many organizations still lack comprehensive training programs to enhance employee awareness (IASM, 2022). Moreover, security management awareness can help mitigate the impact of unforeseen events while averting threats and hazards. Therefore, security management is a crucial part of any organization's overall effort to preserve the safety of its operations and, consequently, the safety of its workers (Beesy papers, 2023). Furthermore, according to Brodowics (2024), the field of security management faces many difficulties. Technological advancements and increasingly complex intrusion techniques require the use of modern security systems in conjunction with more skilled and security-aware individuals. Security concerns are becoming a top priority due to the increase in workplace connections. Organizations sharing internal information online may now face security issues beyond their primary goals. Similarly, Burge (2023) posits that it is an essential part of corporate operations, especially in the present day when businesses frequently deal with various security-related issues. Thus, the threats facing organizations today are multifaceted and constantly evolving. On the other hand, awareness and practices of security management vary significantly across different regions and sectors. According to a study by Alhassan et al. (2020), organizations in developed countries demonstrate a higher level of awareness regarding security threats and management strategies compared to those in developing regions. This gap poses a risk, as human error remains one of the leading causes of security breaches. (Verizon, 2023). Security management practices are diverse and often tailored to the specific needs of an organization. A study by Smith and Jones (2021) categorizes security management practices into three main areas: physical security, information security, and personnel security. While each area necessitates unique strategies and approaches, a cohesive security framework requires their integration. Moreover, the study by Fuentes and Almonte (2021) revealed that all indicators of security policies and procedures, preparedness, efficiency, and effectiveness are significant among stakeholders of Laguna Polytechnic University. Several pieces of literature present the importance of security management and elaborate on the challenges and threats due to technological advancement that led the management to consider security as its top concern. Such

a scenario inspired the researcher to conduct a study to assess current security personnel's awareness and practices of security management. The aim was to develop a proposed action plan that would enhance the respondents' performance and contribute to the achievement of the company's security management goals and objectives.

2. LITERATURE REVIEW

Awareness on Security Management

Awareness on security management encompasses the policies, procedures, and technical measures designed to protect an organization's assets, including information, personnel, and infrastructure. Awareness of security management is crucial in mitigating risks associated with data breaches, cyberattacks, and other security threats. This review explores scholarly and contemporary literature on the importance, challenges, and effectiveness of security management awareness in various contexts. Alqahtani et al. (2022) highlight that increased awareness leads to improved adherence to security policies and a reduction in human-related security incidents. They assert that awareness programs should be continuous and adaptive to address evolving threats and technological advancements. The report suggests that organizations with comprehensive training and clear policies tend to experience fewer security breaches. However, the effectiveness of these programs depends on ongoing evaluation and adaptation to emerging threats. Johnson (2020) contends that awareness is not synonymous with instruction. Simply put, awareness presentations aim to draw attention to security. Presentations on awareness are meant to help people identify and address security issues. In a teaching context, the student plays a more active role; in awareness exercises, the learner is the information provider. Using eye-catching packaging to reach a wide audience is essential to raising awareness. With the aim of enhancing knowledge and abilities to support job performance, training is more structured.

As stated in Mimecast (n.d.), to lower user risk, effective security awareness training emphasizes involving today’s workforce. A lot of security awareness training programs give instruction in one-off sessions that are either forgettable or overly informational, ignoring basic practices in teaching. Employees' hectic schedules require consistent and small doses of training to ensure retention. Most importantly, comedy and positive reinforcement are more effective in helping people remember crucial security subjects than monotonous or fear-based messaging.

Practices on Security Management

The role of security personnel and management in industrial settings has garnered increased attention recently, particularly in large manufacturing firms such as Asia Brewery, Inc. The security practices are vital in mitigating risks, safeguarding assets, and ensuring a safe working environment. Nevertheless, the Asia Brewery, Inc., security management immediately responded to any minor events breaching company protocol to preempt penetrating physical defense, cyber-attacks, and safety concerns. Recent studies emphasize the shift from traditional security approaches to integrated security management systems in industrial environments. According to Dela Cruz et al. (2021), the adoption of technology-driven solutions such as CCTV surveillance, access control, and incident reporting software has been instrumental in enhancing security personnel efficiency and accountability in Philippine

manufacturing plants. These practices align with the organizational objectives of Asia Brewery, Inc., which has reportedly invested in digital security infrastructure to minimize losses and prevent unauthorized access (Santos & Lim, 2022). The practices of security personnel are closely linked to their training and continuous professional development. Bautista (2020) highlighted that regular upskilling, including scenario-based drills and crisis management workshops, contributes to improved response times and decision-making during emergencies. Asia Brewery, Inc. has been noted for implementing quarterly training modules to ensure its security staff are well-prepared for both internal and external threats (Asia Brewery, Inc. Annual Report, 2023). Practices of security management require not only operational expertise but also strong leadership. A study by Lee and Tan (2022) found that participative management styles, where security managers involve personnel in decision-making and feedback processes, lead to higher morale and compliance with security protocols. Asia Brewery, Inc.'s management reportedly employs regular performance reviews and open communication channels, fostering a proactive security culture (Villanueva, 2023). Despite advancements, challenges remain. Resource constraints, evolving threat landscapes, and the integration of third-party security agencies pose hurdles to the consistent implementation of best practices (Garcia & Yu, 2021). However, partnerships with reputable security service providers and ongoing investment in security technology have been identified as key opportunities for continuous improvement within companies like Asia Brewery, Inc. It concluded that improvements toward the professionalization and modernization of security practices in industrial firms must recommend adopting technology, emphasizing training, participative management, and strategic partnerships. Therefore, this research highlights central themes such as the autonomy of security practices, competence and skill development, and the relatedness and team support of security personnel.

Security Policies and Protocols

An organization’s policies and processes are vital components. Policies and procedures work together to create a schedule for daily operations. They guarantee adherence to legal and regulatory requirements, provide direction for making decisions, and optimize internal procedures (Power DMS, 2020). As stated in Faster Capital (2024), strong policy enforcement measures are essential for effective regulation. It is impossible to overestimate the significance of policy enforcement, be it in the fields of financial markets, data privacy, or environmental protection. It serves as the foundation upon which the entire regulatory system is built, providing it with the necessary strength to ensure compliance. More broadly, it ensures that the rules are consistently and equitably applied to all parties involved. A security policy is a document outlining the rules, expectations, and approach for maintaining data confidentiality, integrity, and availability. It outlines an organization's general security goals and principles and addresses specific issues like remote access or Wi-Fi use. It is often used alongside standard operating procedures to achieve security goals, addressing the “what” and “why” of security practices (Grimmick, 2023).

Training and Adaptation

As stated in Cybersafe (2023), security awareness training is the process of teaching people how to recognize, identify, and prevent cyber dangers. The ultimate goal is to prevent or mitigate harm to both the company and its stakeholders, as well as to reduce human cyber risk. Security awareness training is the process of educating individuals on how to comprehend, recognize, and avoid cybersecurity dangers.

The ultimate goal is to avoid or mitigate harm to the firm and its stakeholders while also lowering human cyber risk.

Security awareness training is an essential component of any organization's defense strategy against cybersecurity attacks. Organizations can greatly minimize their vulnerability to cyberattacks by teaching staff about the importance of security, hacking techniques, and risk mitigation strategies. This detailed resource digs into the fundamentals of security awareness training, highlighting its significance, components, and best practices for implementation (Divyaja, 2024).

Knowledge and Sharing

Recent studies emphasize that knowledge sharing serves as a fundamental mechanism for cultivating a security-conscious organizational culture. According to Alshaikh et al. (2020), organizations that promote open communication channels and collaborative learning tend to demonstrate higher levels of employee awareness regarding cybersecurity threats. Businesses recognize security awareness as the most essential component in reducing the risk of information security breaches. Knowledge sharing entails more than just passing along facts. It is a culture of sharing information that allows people to accomplish their jobs more effectively. It can occur through official techniques such as meetings, documentation, and training sessions, or informally through conversations and emails (Guthrie, 2024). Knowledge sharing is a crucial component of any company to reap the benefits of improved performance, decision-making, and transparency. Thus, it is equally critical to disseminate knowledge about ISRM procedures. Similarly, Kumar and Sharma (2020) highlight that organizations implementing knowledge-sharing strategies report reduced security breaches owing to increased employee vigilance.

Autonomy on Security Practices

According to Domas (2023), autonomy, like autonomous, is a contentious issue with uncertain implications. The name is taken from Greek and is a mix of the word's autos, means "itself" and nomos, means "law. In literary terms, autonomy implies that an independent being may impose its own standards on itself and is self-determined. When it comes to a person or a group of individuals, these notions are unquestionably valid; but when it comes to platforms and systems, the situation becomes slightly more problematic. Security autonomy allows companies (or governments) to regulate the security of the technologies they utilize. It is understandable that corporations desire to take charge of their own cybersecurity destiny. Autonomy grows in interaction and is affected by people's conceptions of themselves in relation to their surroundings. As a result, we can discuss perceived autonomy, which is a multifaceted, dynamic, and relational term (van Loon et al. as cited in Sanberg et al., 2022).

Competence and Skill Development

According to Sari (2023), modern business practices now emphasize the significance of corporate governance, which highlights the need for efficient oversight and responsibility inside companies. Over time, the dynamics of corporate governance have undergone significant evolution due to a multitude of variables, including globalization, technology breakthroughs, regulatory reforms, and shifting stakeholder expectations. This means that to ensure organizational sustainability, reduce risks, and promote long-term value generation, it is essential to comprehend and improve corporate governance systems. In addition, the ability of an authority to accomplish its goals, handle its finances, and uphold

the confidence of the people it serves is fundamentally dependent on good governance. Stronger decision-making, more careful consideration of options, and improved long-term planning are all encouraged by good governance. A firm must, then, be founded in line with the fundamentals of good governance, have competent and efficient financial management, and adhere to all applicable laws. In addition, the establishing authority needs to maintain appropriate systems to guarantee efficient supervision and responsibility for any alternative delivery methods it has used (CIPFA, 2023). A security program is meaningless without the formalization and, more importantly, the execution of governance. If not, it would depend on having the right programmers to run it. Should the individuals depart or the degree of assistance fluctuate, the security initiative may come to an end.

Relatedness and Team Support

Security programs are only as good as their employees, and leaders are only as effective as their teams. So, if teams get disengaged and burnt out as a result of higher workloads, bad management, or a lack of support, it has a knock-on effect throughout the business. The security program will stagnate, leaving leaders ill-equipped to achieve its primary purpose of protecting the business (Henriquez, 2022). Moreover, as stated in Standley System Staff (2024), security is a team effort. Historically, job responsibilities were limited to certain departments. However, recently, the distinction between job duties and responsibilities has blurred. Fewer people may rely on their departments to determine what is and is not part of their duties.

Research Literature

The importance of security management.

The dynamic nature of threats in the 21st century needs tailored security solutions. The adoption of customized security management enables organizations to address industry-specific risks and respond flexibly to unforeseen events. As noted by Smith et al. (2020), organizations that implement adaptive and context-sensitive security measures are better positioned to avert hazards and minimize the impact of disruptions. Security management involves constantly checking for risks, providing regular training, and using advanced technology tools like AI-powered cameras, drones, and real-time monitoring systems such as biometric and facial recognition machines. These measures collectively foster a proactive security culture that can detect and neutralize threats before they escalate (Miller & Roberts, 2020). In addition, security management is pivotal in ensuring organizational resilience. A study by Alshaikh (2020) found that organizations with mature security management practices were significantly more resilient during cybersecurity incidents, experiencing less downtime and financial loss compared to those with ad hoc approaches. As organizations rapidly shifted to remote work, those with established security protocols were better equipped to manage new vulnerabilities and maintain operational continuity (Kraus et al., 2020).

Furthermore, Jeanpert et al. (2021) argue that the topic of how to handle customer complaints is still up for dispute, despite the consensus that handling them is essential for businesses. Direct human connection may no longer be required in the recovery process, as an increasing number of studies demonstrate the positive effects of digital complaint channels on customer behavior and satisfaction**.** Smith and Brooks (2020) explain that by managing security risks, one can gain a deeper comprehension

of the types of security threats and how they interact with one another at the individual, organizational, and community levels.

Challenges in Security Management

Security management is dealing with new problems from natural threats caused by the complicated nature of modern technical systems, which can operate on their own without human input; mixed threats that arise from random coincidences and interactions of different factors that are usually safe on their own; and combined risks from the buildup of dangerous effects, each of which is acceptable when considered alone (Michalski, 2021).

3. METHODOLOGY

Research Design

This study utilized a descriptive-correlational research design. The study employed statistical techniques to enhance its reliability and credibility. This entails collecting information without manipulating the environment or changing it in any way. It is used to collect information on the current state of the phenomenon to define "what exists" in terms of factors or conditions in a particular situation. The study of Lee and Kim (2020) demonstrated the use of large-scale surveys to assess the prevalence of mental health issues among adolescents. The descriptive statistics provided a snapshot of current mental health trends, while correlational analysis explored associations with demographic factors.

Research Locale

This study focused on the security management in Asia Brewery, Inc., located at KM. 43, ABI Complex, Barangay Sala, Cabuyao City, Laguna 4025, is known as one of its major manufacturing hubs. This facility focuses on brewing, bottling, and packaging operations. These plants are equipped with modern technology and are situated in key industrial zones to optimize production and logistics. The researcher has access to the respondents in the said company as a corporate security and safety specialist.

Respondent of the Study

The respondents are a composite of college, vocational, senior high school, and high school graduate skilled licensed security personnel. Their current strength is composed of 133 security personnel. Likewise, the respondents were selected through utilizing a simple random sampling test study. The sample size will be computed using the Raosoft sample size calculator. Using a confidence level of 95% and a margin of error of 5% quantifies the range within which the true value is expected as a balance between precision and feasibility (Singh & Masuku, 2020).

Sampling Design

A simple random sampling (SRS) was used in this study, which is a method where each member of a population has an equal likelihood of being chosen for the sample, ensuring representativeness and reducing selection bias. In practice, researchers randomly select respondents from a complete list of the population, often using the fishbowl technique or other randomization tools. This sampling approach is favored for its ease of implementation and statistical robustness, making it particularly useful for studies

requiring generalizable results. Simple random sampling allows for the application of various statistical techniques. As highlighted by recent studies, SRS is pivotal in achieving a representative sample of the target population. According to Johnson et al. (2021), SRS guarantees that every individual in the population has an equal probability of selection, which is critical for generalizing findings beyond the sample. Likewise, Chen and Liu (2022) showed through simulation studies that SRS was better than non-random methods at providing accurate estimates, especially in large social science surveys.

Instrumentation

The researcher conducted a face-to-face paper survey and utilized a self-constructed questionnaire written in English and translated into Filipino to collect the needed primary data. To assess the manifestation of the level of awareness and practices on security management, the survey questionnaire is divided into three primary sections. Part 1 focuses on the demographic profile of the respondents, while Part 2 measures the level of awareness among the security personnel on security management. Part 3 is about the practices of security management at Asia Brewery, Inc. Furthermore, the tool or instrument to be used will be validated by the experts in management, statistics, and research.

Validation and Scoring

Three experts in the relevant field validated the questionnaire, ensuring its reliability and relevance to the study objectives. Additionally, the study aimed to ascertain the respondents' understanding of the security personnel and management practices implemented by agency deployed at the Asia Brewery, Inc. Then the following adapted numerical rating, numerical range, categorical response, and verbal interpretation must be properly evaluated based on the result of the study. Moreover, a pilot test of the research instrument was covered by fifteen (15) respondents who were not involved in the study's real. The validators and research advisers received the findings of the pilot test and used them to support their approval of the researcher's finalization of the questionnaire. To determine the validity of the questionnaire and the data gathered, it must be calculated through the Cronbach alpha test to measure its reliability and consistency before proceeding with the final survey. Furthermore, the assigned statistician used the Kruskal-Wallis H-test, Mann-Whitney U-test, and Spearman Rho based on the appropriate questionnaire survey results. Subsequently, in comparison, it uses a Dwass-Steel-Critchlow-Fligner pairwise comparison.

Table A. Likert Scale for level of awareness on security management

Numerical Rating	Numerical Range	Categorial Response	Verbal Interpretation
4	3.25 – 4.00	Strongly Agree (SA)	Very Much Aware
3	2.51 – 3.24	Agree (A)	Much Aware
2	1.75 – 2.50	Disagree (DA)	Less Aware
1	1.00 - 1.74	Strongly Disagree (SD)	Not Aware

Table B. Likert Scale for practices on security management

Numerical Rating	Numerical Range	Categorial Response	Verbal Interpretation
4	3.25 – 4.00	Strongly Agree (SA)	Always Practiced
3	2.51 – 3.24	Agree (A)	Practiced
2	1.75 – 2.50	Disagree (DA)	Rarely Practiced
1	1.00 - 1.74	Strongly Disagree (SD)	Never Practiced

Data Gathering Procedures

This section outlines the systematic steps for collecting data regarding the demographic profile of the security personnel, the level of awareness, and its practices on security management among security personnel in Asia Brewery, Inc. In the preparation phase, the aim is for approval and coordination; the researcher seeks permission from the appropriate authorities to conduct a survey in Asia Brewery, Inc. The security management must approve it and ensure proper coordination. The goal and importance of the study must be communicated in a clear and concise manner. Nevertheless, asking for favorable support in facilitating the survey. Afterwards, the proponents will be developing a survey instrument, designing the survey questionnaire based on the research objectives, and incorporating items aligned with the Social Cognitive Theory and Self-Determination Theory. The questionnaire included Likert scale questions and other relevant sections. The next phase is pretesting, or pilot testing the instrument, conducting a survey with 15 security personnel assigned from the different company to assess the clarity, reliability, and validity of these, and then refining the survey instrument based on feedback.

The second phase is data collection, which involves the recruitment of respondents. We need to identify potential respondents through simple random sampling to ensure they meet the inclusion criteria. The researcher then distributed the questionnaire to respondents using one of the following methods: During on-site administration, the researcher distributed physical copies of the questionnaire and guided respondents in filling them out. To ensure the accuracy and completeness, the researcher provided a brief orientation to respondents on how to answer the questionnaire. Check completed questionnaires for missing or inconsistent responses before concluding the session.

The third phase is the ethical considerations; the informed consent will be provided to the respondents with an informed consent form detailing the study's purpose, confidentiality of data, voluntary participation, and the right to withdraw at any time. We will ensure anonymity and confidentiality by anonymizing all collected data and keeping respondents' responses confidential to protect their identity. Comply by following ethical guidelines and obtaining any necessary permits from the management.

The last phase is the data organization and validation. For data encoding, the researcher encoded the responses into statistical software (e.g., SPSS, Microsoft Excel) or a database for analysis. The encoded data were reviewed for errors, duplicates, or incomplete entries. Validate data through random checks or cross-referencing with observations (if applicable). Afterwards was the analysis and interpretation phase; it needs to analyze the data using descriptive statistics to determine the level of security management and

its practices and use inferential statistics to explore the relationship between the level of awareness of security management and its practices. This procedure ensures the systematic collection of reliable and valid data, providing insights into the awareness and practices on security management among security personnel.

Treatment of Data

This study will use the following statistical tools:

1. Percentage and frequency to determine the respondents' profiles.

2. Weighted means were used to describe the respondents' level of awareness and practices of the security management agency deployed in Asia Brewery, Inc.

3. Kruskal-Wallis H-test and Mann-Whitney U-test were used to measure the test of significant difference in awareness and practices of security management across each demographic profile.

4. Spearman's Rho was used to measure the significant relationship between awareness and practices of security management in Asia Brewery.

Ethical Consideration

The researchers completed the study while keeping ethical factors in mind, such as confidentiality, quality, and the protection of human subjects. Every participant was required to answer the questionnaire precisely based on their experience and knowledge in the security profession. Through voluntary participation, the respondents agreed to take part in the research without any coercion or pressure. They also received information about the research's purpose, benefits, and risks. They also assure the researcher of absolute confidentiality and require them to sign a consent form before collecting any data. The researcher will also tell participants they can join or leave the study at any time. The participants shall be informed about the outcomes and implications of the research, and they have authorized the research report or publication if they wish. Rest assured that the personal information and other sensitive data entrusted were used with due diligence for the sole purpose of this research and were treated with utmost confidentiality in accordance with the Data Privacy Act of 2012.

4. RESULTS AND DISCUSSION

1. The demographic profile of the security personnel in terms of:

1.1. years of stay;

In Table 1.1 result indicates that most security personnel have been with the company for shorter durations; the first 1-5 years (55.6 %) is the highest retention, while 20 and above years of stay is the lowest result of security personnel retained in the company, or having 5.1% on the research. These signify either high turnover or rendered retransfer of post assignment, career enhancement, and absorption by Asia Brewery, Inc. as their regular employee. According to the U.S. Bureau of Labor Statistics (2023), the median tenure for protective service occupations, including security guards, is approximately 3.1 years, which is notably lower than the national average for all occupations. The finding suggests that short-term

tenure is a common phenomenon in the industry. As per Smith & Lee (2021), multiple factors contribute to the relatively short tenure among security personnel. These include job satisfaction, compensation, work environment, and opportunities for advancement. In a relatively recent instance, a company deployed security personnel who voluntarily resigned for various reasons. However, some companies continue to retain a few security personnel after they have voluntarily resigned.

Table 1.1

The Demographic Profile of the Security Personnel in terms of Years of Stay.

Demographic Profile	Frequency	Percentage	Rank
1 to 5	55	55.6	1
6 to 10	17	17.2	2
11 to 15	13	13.1	3
16 to 20	9	9.1	4
21 and above	5	5.1	5
Total	99	100.0	

1.2. current position;

In Table 1.2, it is shown that the number of female guards is only 16.2% compared to the number of male guards, which is 83.8%. This highlights the necessity of an agency contract between the management of Asia Brewery, Inc., and the required security personnel stationed in the area. Globally, the security services sector has traditionally been male-dominated. According to the International Labor Organization (ILO, 2020), women make up less than 20% of the private security workforce worldwide. In the Philippines, the situation mirrors global trends. Studies have shown that female security guards are significantly underrepresented. A report by the Philippine National Police Supervisory Office for Security and Investigation Agencies (PNP-SOSIA, 2022) indicated that women account for only 15%–18% of the total security guard population nationwide. To say it another way, male guards are largely needed in the security industry compared to female guards in terms of physical security postings or assignments, like Asia Brewery, Inc. However, other companies, like call centers, malls, and other industrial companies with CCTV operators, hire them as a priority for smooth security operations.

Table 1.2

The Demographic Profile of the Security Personnel in terms of Current Position.

Demographic Profile	Frequency	Percentage	Rank
Lady Guard (LG)	16	16.2	2
Security Guard (SG)	83	83.8	1
Total	99	100.0	

1.3. frequency on training session, and

Table 1.3 shows that the majority of the security personnel attended five times in their training sessions, which is 60.6%, categorized as the highest percentage in training frequency. This high training frequency can positively impact security readiness and response capability. The lowest training frequency, with an average of 3%, suggests that there may be limited access, schedule conflicts, oversights in training distribution, or newly transferred security personnel who have been with the company for more than a year. These security personnel may be at risk of lacking updated knowledge on evolving security protocols, as stated by Kumar & Patel (2022). As noted by Garcia (2022), security systems such as surveillance, access control, and cybersecurity require specialized knowledge that must be regularly updated. Security personnel who participate in frequent training sessions are better equipped to utilize new tools, interpret data accurately, and maintain operational efficiency. Aligned with the perception of Smith et al. (2021), regular training sessions ensure security personnel remain updated on the latest instructions, protocols, technologies, and best practices, contributing to more effective incident management and prevention. The agency deployed in Asia Brewery, Inc., such as St. Thomas Security and Investigation Agency, has proposed a monthly training course for its personnel at the company. The purpose of this training is to enhance and update the knowledge of the security personnel. This training session covers a specific topic each month, such as report writing, telephone etiquette, leadership traits, code of conduct, and security awareness. By taking these courses each month, they enhance their knowledge and skills relevant to their profession. Their agency and the company also allocate budgets for their snacks and meals during their lessons. This program emphasizes familiarizing and updating them on access control policy, knowing the company rules and regulations, understanding how to handle critical scenarios, assisting victims in any accidents or incident situations for first aid, and knowing how to do fire drills and responses in times of pickets or rallies.

Table 1.3

The Demographic Profile of the Security Personnel in terms of Frequency of Training Session.

Attended per Year	Frequency	Percentage	Rank
Once	15	15.2	2
Twice	3	3.0	5
Three times	11	11.1	3
Four times	10	10.1	4
Five times	60	60.6	1
Total	99	100.0	

1.4 educational background?

In Table 1.4, the largest group in the sample survey consists of junior high school graduates, accounting for 51.5% of the population. It indicates that the majority of respondents reached only up to junior high school. It shows a significant educational gap that may influence employment opportunities, literacy levels, or access to higher education. Furthermore, it is the company's highest education requirement based on RA5487 (Para 5 Qualification required). The lowest group, comprising only 9.1% of technical-vocational courses, underutilizes or lacks access to skills-based programs, which could pose

a concern if the goal is to promote employable skills in the workforce. These results are concerning, as technical-vocational education and training (TVET) graduates are often well-equipped for the labor market, particularly in sectors experiencing skills shortages (International Labor Organization, 2020). Lopez & Tan (2021) have noted a shift towards competency-based hiring, which increasingly values practical skills and experience in addition to formal education. At Asia Brewery, Inc., the minimum educational requirements for supervisory positions are as follows: a college graduate with a Certified Security Professional (CSP) is considered an advantage, while security personnel must be high school graduates with a security license and no derogatory records. However, those who possess skills and complete their baccalaureate degree have an advantage. Over time, they have a chance to promote or prioritize hiring in Asia Brewery, Inc. as a regular employee in the company. Furthermore, it concluded that the demographic profile of security personnel is crucial in understanding workforce dynamics, training needs, and overall organizational success. As per Klein & Molloy's (2020) evaluation, employee tenure, training frequency, educational background, and gender composition are emphasized in the security sector.

Table 1.4

The Demographic Profile of the Security Personnel in terms of Educational Background.

Demographic Profile	Frequency	Percentage	Rank
College Graduate	17	17.2	2
Senior High School	11	11.1	3.5
Junior High School	51	51.5	1
Under- Graduate	11	11.1	3.5
Technical -Vocational	9	9.1	5
Total	99	100.0	

2. What is the level of awareness in security management among security personnel in Asia Brewery, Inc. in terms of:

2.1 security policies and protocols

In Table 2.1, statement number 1 (the security policies and protocol are clearly communicated, and I am familiar with it) is the highest mean result of 3.87. This result indicates a strong awareness and communication of policies among the security personnel. The initial efforts by Asia Brewery, Inc. in policy dissemination and orientation have been effective. The Asia Brewery, Inc.'s initial efforts in policy dissemination and orientation have yielded a low mean score of 3.16 under the number 5 category, indicating that the tools and technologies we utilize effectively mitigate security risks. This score corresponds to rank number 5, and its verbal interpretation is "Very Much Aware." This result implicates that strong, awareness-communicated policies provide a solid foundation for effective security practices. However, the perceived limitations of technology tools could hinder full implementation of these policies in real-world scenarios. In summary, while all aspects are rated "Very Much Aware", the data shows a gradual decrease in mean from communication and policy clarity to the perceived effectiveness of tools, suggesting a potential focus area for future training or resource allocation. Hence with overall verbal interpretation of "Very Much Aware" level of understanding across all measured aspects of security policies and protocols, as indicated by an overall weighted mean of 3.57 with a standard deviation of 0.45.

Furthermore, other companies should invest in updated technologies to ensure consistent training on tool usage and gather feedback from users to bridge this perception gap. An additional study by AlHogail (2020) suggests that effective security policies need to be comprehensive, adaptable, and clearly communicated to ensure organizational compliance. Chen et al. (2021) conducted a parallel study that highlights the crucial role of efficient dissemination mechanisms in ensuring the success of security policies by promoting understanding and adherence among stakeholders. Likewise, the study of Zhang et al. (2021) proposed a machine learning-based framework that dynamically updates security policies based on emerging threats, thereby enhancing responsiveness and reducing manual effort.

The overall impact of the findings demonstrates that Asia Brewery, Inc. has solid policies and procedures in place. The company's frontliners or security personnel consistently implement this awareness program to mitigate risk and preempt losses. Throughout the business, both agency-deployed and management personnel have experienced an increase in trust and confidence. However, those violators attempting to violate the said policies and protocols are facing consequences and due process. Currently, the security management is actively enforcing these practices to prevent pilferage and to discipline employees who engage in delinquent activities within the company.

Table 2.1

The Level of Awareness in Security Management among Security Personnel in Asia Brewery, Inc. in terms of Security Policies and Protocol

Statement	Mean	SD	Verbal Interpretation	Rank
1. The security policies and protocol are clearly communicated, and I am familiar with it.	3.87	0.34	Very Much Aware	1
2. The security policies and protocols are easy to follow and are updated regularly to address new threats.	3.79	0.50	Very Much Aware	2
3. The security policies and protocol adhere to standard operating procedure of proper reporting of incident.	3.70	0.65	Very Much Aware	3
4. The security personnel regularly check and update software and devices to avoid security vulnerabilities of the company.	3.32	0.91	Very Much Aware	4
5. The tools and technologies we use are effective in mitigating security risks.	3.16	0.75	Very Much Aware	5
Overall Security Policies and Protocol	**3.57**	**0.45**	**Very Much Aware**	

Legend: 3.25-4.00 Very Much Aware, 2.51-3.24 Much Aware, 1.75-2.50 Less Aware, 1.00-1.74 Not Aware

2.2 training and adaptation; and

This Table 2.2, statement number 1 (The training programs provided by the organization are effective about duties and responsibilities), is ranked under number 1 with a

total mean of 3.74 and a standard deviation of 0.53, with a result of "Very Much Aware." In other words, the company aligns its training programs with its duties and responsibilities effectively. The company ranks lowest at number 4, with a mean score of 2.92, a standard deviation of 1.12, and a verbal interpretation of "Much Aware". The results reveal that security personnel at Asia Brewery, Inc. exhibit a "Very Much Aware" level with an average mean of 3.56 regarding training and adaptation within security management. This implies that the respondents positively perceive and are highly aware of the training provisions and their adaptability as they deem those trainings effective as they perform their duties and responsibilities.

This finding suggests that there are certain areas where training and career development programs could be more effectively promoted. Without consistent encouragement for continuous learning, security personnel may plateau in their skill growth, fall behind on evolving security practices, or feel undervalued. Such conditions can ultimately impact security personnel's motivation, adaptability, and job satisfaction. Apparently, Johnson (2024) emphasizes that fostering a culture of continuous learning is fundamental for maintaining a skilled and adaptable workforce in security management. In complex security environments, static skill sets can quickly become obsolete, underscoring the necessity for ongoing training initiatives. Continuous learning not only enhances technical competencies but also promotes critical thinking and problem-solving skills essential for effective security operations.

The St. Thomas Security Agency reportedly offers training programs for their security personnel, including a study now and pay later plan. Upon the deployment of said personnel, the agency will gradually deduct their total program expenses. Security management sets aside money specifically for the training program during the company's actual deployment. They will use those funds to cover their meals and snacks until their training is complete. All training courses are applicable for long-term purposes to develop trusted personnel and build a strong security organization as a whole. Furthermore, both the agency and security management of ABI conducted training programs to minimize turnover.

Table 2.2
The Level of Awareness in Security Management among Security Personnel in Asia Brewery, Inc. in terms of Training and Adaptation

Statement	Mean	SD	Verbal Interpretation	Rank
1. The training programs provided by the organization is effective pertaining to duties and responsibilities.	3.74	0.53	Very Much Aware	1
2. There is a clear understanding of the different roles and tasks to be carried out at works.	3.73	0.53	Very Much Aware	3
3. The training materials and resources are easy to understand and apply.	3.75	0.52	Very Much Aware	2

4. The organization encourages continuous learning and professional development.	2.92	1.12	Much Aware	5
5. The feedback mechanism after training programs helps me improve and adapt effectively.	3.67	0.55	Very Much Aware	4
Overall Training Adaptation	**3.56**	**0.47**	**Very Much Aware**	

Legend: 3.25-4.00 Very Much Aware, 2.51-3.24 Much Aware, 1.75-2.50 Less Aware, 1.00-1.74 Not Aware

2.3. knowledge sharing?

In Table 2.3, statement number 1 (The tools and platforms provided by the organization facilitate effective knowledge sharing.) is rank number 1 with a mean of 3.75, a standard deviation, and “Very Much Aware” of its verbal interpretation. This assessment underscores the general consensus that security personnel have mutual knowledge sharing within the company. The lowest rank is tied between numbers 4 and 5: No. 4 - The organization recognizes and rewards employees who actively engage in knowledge sharing with others, and No. 5 - Knowledge sharing is part of our work culture to share ideas and experiences with others. The results show a mean score of 3.62, with a standard deviation of 0.68, which is verbally interpreted as “Very Much Aware.” This result implies that security personnel are generally aware that knowledge sharing is encouraged, but the lower score may signal that this practice is not fully embedded or actively reinforced in the daily workflow.

The overall mean of 3.68, with a "Very Much Aware" verbal interpretation, indicates a positive perception of knowledge sharing practices. This perception is built upon five key indicators: the effectiveness of organizational tools and platforms, the existence of a structured documentation system, management's active participation, recognition and rewards for knowledge sharing, and the integration of knowledge sharing into the work culture. Similarly, Johnson et al. (2021) found that organizations with strong knowledge-sharing cultures among security personnel experienced fewer security breaches. It emphasizes that trust, openness, and communication channels are critical enablers of effective knowledge exchange. Further study by Lee and Kim (2020) argues that security personnel who actively share information foster a collective understanding of potential threats, which enhances the organization's overall security posture.

Table 2.3
The Level of Awareness in Security Management among Security Personnel in Asia Brewery, Inc. in terms of Knowledge Sharing

Statement	Mean	SD	Verbal Interpretation	Rank
1. The tools and platforms provided by the organization facilitate effective knowledge sharing.	3.75	0.58	Very Much Aware	1

2. There is a structured system in place for documenting and sharing knowledge within the organization.	3.68	0.59	Very Much Aware	3
3. Management actively participates in and supports knowledge sharing initiatives.	3.73	0.49	Very Much Aware	2
4. The organization recognizes and rewards employees who actively engage in knowledge sharing with others.	3.62	0.68	Very Much Aware	4.5
5. Knowledge sharing is part of our work culture to share ideas and experiences with others.	3.62	0.60	Very Much Aware	4.5
Overall, Knowledge Sharing	**3.68**	**0.45**	**Very Much Aware**	

Legend: 3.25-4.00 Very Much Aware, 2.51-3.24 Much Aware, 1.75-2.50 Less Aware, 1.00-1.74 Not Aware

3. What practices on security management in terms of security personnel in Asia Brewery, Inc. in terms of:

3.1 autonomy on security practices;

In Table 3.1, statement number 1 is: "I feel confident in making decisions regarding security practices in my role." The statement has a mean of 3.78 and a standard deviation of 0.49. **"**Always Practiced" is its verbal interpretation and ranked as the highest result. It indicates that the security personnel possess a strong sense of self-efficacy and decision-making autonomy, which is essential for frontline roles that require swift, independent action in emergencies. According to Al-Mawali et al. (2022), employee self-confidence in operational decision-making correlates significantly with performance in high-risk settings like security, especially when employees are well-trained and trusted by their organizations. Furthermore, Wu, Parker, & de Jong (2021) emphasize that autonomous motivation and perceived competence contribute to proactive security behavior in organizations, reducing reliance on top-down command structures and improving organizational resilience. While the lowest result under statement number 5 (the management promotes and recognizes the initiatives of security personnel on autonomy on security) has a mean of 3.26, a standard deviation of 0.82, and a verbal interpretation of "Always Practiced," it is marked as number 5. The overall mean of 3.65, interpreted as "Always Practiced," indicates that personnel consistently experience a high level of independence in their security-related duties. While still within the "Always Practiced" range, the lower mean and higher standard deviation indicate a potential area for improvement. The other four statements show that the security personnel feel that they are given autonomy, but the company could improve in recognizing the security personnel independent security initiatives. The result implicates a perceived gap or consistency in how management acknowledges and reinforces autonomous efforts among personnel. Some employees may feel that their initiative is not sufficiently recognized or rewarded, potentially impacting motivation over time. According to Bari, Fan, and Ullah (2021), recognition of employee initiatives significantly

affects job satisfaction and organizational commitment in operational roles. A lack of acknowledgment, even when autonomy is allowed, can diminish the psychological benefits of empowerment. In addition, Decuypere and Schaufeli (2020) highlight that managerial support and positive reinforcement are essential for sustaining proactive behaviors. Without this reinforcement, even confident and competent employees may feel undervalued or disengaged.

Table 3.1

Practices on Security Management in terms of Security Personnel in Asia Brewery, Inc. in terms of Autonomy on Security Practices

Statement	Mean	SD	Verbal Interpretation	Rank
1. I feel confident in making decisions regarding security practices in my role.	3.78	0.49	Always Practiced	1
2. The management provides adequate support to exercise my autonomy in security decisions provided legal and valid reasons.	3.77	0.49	Always Practiced	2
3. The organization encourages autonomy by providing me with the freedom to address security threats as I see fit.	3.75	0.44	Always Practiced	3
4. I have the autonomy to implement security practices that I believe are effective in critical and emergency situations.	3.70	0.50	Always Practiced	4
5. The management promotes and recognizes the initiatives of security personnel on autonomy on security.	3.26	0.82	Always Practiced	5
Overall Autonomy on Security Practices	**3.65**	**0.39**	**Always Practiced**	

Legend: 3.25-4.00 Always Practiced, 2.51-3.24 Practiced, 1.75-2.50 Rarely Practiced, 1.00-1.74 Never Practiced

3.2 competence and skill development; and

The results presented in Table 3.2 indicate that the first statement, "I feel confident in my ability to perform my job tasks competently," ranked highest, with a mean score of 3.90, a standard deviation of 0.30, and a verbal interpretation of "Always Practiced." This study connects a high level of self-esteem among security personnel with independent decision-making and lower error rates in addressing unusual events. According to Geldenhuys, Laba, & Venter (2020), employee confidence in their skills leads to higher engagement and job performance, especially in roles involving critical responsibility like security services. Additionally, Park, Newman, et al. (2020) discovered that employees who perceive themselves

as competent are more likely to engage in proactive behaviors, thereby contributing to workplace safety and operational resilience. Statement number 5, 'I regularly receive feedback that helps me improve my skills and competencies,' was marked as the lowest result under rank 5, with a mean of 3.53 and a standard deviation of 0.69, interpreted verbally as 'always practiced.' This result implicates inconsistency in feedback practices, where some security personnel may receive regular, constructive feedback while others do not. This inconsistency might lead to slower skills improvement, unclear performance expectations, and reduced motivation for continuous career growth among security personnel. The overall mean of 3.76, interpreted as "Always Practiced," indicates that personnel consistently perceive their skills and development positively. Thus, Asia Brewery, Inc. effectively fosters competence and skill development, with a particular strength in building job confidence and providing relevant training. As stated by Wibowo et al. (2021), feedback is essential for competency development. Timely feedback in security contexts guarantees the correction of errors before they result in breaches or incidents. Supported by Smith et al. (2020), the study demonstrates that continuous feedback positively influences technical skill mastery by providing learners with immediate insights into their performance. Similarly, soft skills such as communication, teamwork, and adaptability are enhanced through reflective feed.

Table 3.2

Practices on Security Management in terms of Security Personnel in Asia Brewery, Inc. in terms of competence and skill development

Statement	Mean	SD	Verbal Interpretation	Rank
1. I feel confident in my ability to perform my job tasks competently.	3.90	0.30	Always Practiced	1
2. The organization provides adequate opportunities for skill development.	3.72	0.54	Always Practiced	4
3. The organization encourages continuous learning and development.	3.80	0.40	Always Practiced	3
4. The skills I develop through training are relevant to my job responsibilities.	3.86	0.43	Always Practiced	2
5. I regularly receive feedback that helps me improve my skills and competencies.	3.53	0.69	Always Practiced	5
Overall Competence and Skill Development	**3.76**	**0.34**	**Always Practiced**	

Legend: 3.25-4.00 Always Practiced, 2.51-3.24 Practiced, 1.75-2.50 Rarely Practiced, 1.00-1.74 Never Practiced

3.3. relatedness and team support?

This Table 3.3 statement number 3 (My contributions to the team are valued and appreciated) marks as the rank number 1 with a 3.73 mean, a 0.45 standard deviation, and a verbal interpretation of

"Always Practiced." This finding implies that when team members feel their input is acknowledged, it strengthens their sense of belonging and motivation to contribute meaningfully to collective security goals. As stated by Henriquez (2022), employee recognition increases engagement and loyalty, particularly in roles that require sustained vigilance and teamwork, such as security. Standley System Staff (2024) asserts that feeling valued is a cornerstone of effective team dynamics, especially in environments where coordination and trust are essential to operational success. Statement number 2 ("There is a high level of trust among my team members.") has the lowest rank with a mean of 3.52, a standard deviation of 0.68, and a verbal interpretation of "Always Practiced." The team consistently practices trust. In the context of security personnel and management, gaps in trust can hinder communication, delay response times, and lead to miscoordination, particularly in high-stakes scenarios In summary, the overall mean of 3.64, interpreted as "Always Practiced," indicates a consistent perception of positive team relatedness and support. Therefore, Asia Brewery, Inc. fosters a positive team environment where contributions are valued and collaboration is effective. However, there is a potential area for improvement in strengthening trust among team members to further enhance overall relatedness and team support. Henriquez (2022) identifies team trust as a foundation for successful collaboration, particularly in high-risk industries where mutual reliance is non-negotiable. Standley System Staff (2024) explains that trust among team members enhances decision-making and problem-solving, emphasizing that even minor breakdowns in trust can lead to operational vulnerabilities. Moreover, trust accelerates the decision-making process by minimizing conflict and misunderstandings. A study by Nguyen et al. (2022) demonstrated that trusted teams are more agile and adaptive, capable of swiftly responding to operational challenges without the delays caused by excessive oversight or mistrust.

Table 3.3

Practices on Security Management in terms of Security Personnel in Asia Brewery, Inc. in terms of Relatedness and Team Support

Statement	Mean	SD	Verbal Interpretation	Rank
1. I feel a sense of belonging within my team.	3.63	0.63	Always Practiced	3
2. There is a high level of trust among my team members.	3.52	0.68	Always Practiced	5
3. My contributions to the team are valued and appreciated.	3.73	0.45	Always Practiced	1
4. My team collaborates well to achieve common goals.	3.70	0.54	Always Practiced	2
5. I feel motivated and inspired by my team's collective efforts and achievements.	3.62	0.55	Always Practiced	4
Overall Relatedness and Team Support	**3.64**	**0.40**	**Always Practiced**	

Legend: 3.25-4.00 Always Practiced, 2.51-3.24 Practiced, 1.75-2.50 Rarely Practiced, 1.00-1.74 Never Practiced

4. Is there a significant difference in the level of awareness and practices of security management when grouped according to a demographic profile?

4.1. The level of AWARENESS of security management when grouped according to demographic profile:

4.1.1 years of stay

In Table 4.1.1, the significant difference in the level of awareness on security management when grouped according to years of stay at Asia Brewery, Inc. The p-values for all four categories (Security Policies and Protocol, Knowledge Sharing, Training Adaptation, and Overall Awareness) are greater than 0.05 ($p > 0.05$). Therefore, the decision is "Failed to reject Ho" (the null hypothesis), indicating that there is no statistically significant difference in the level of awareness across the different years of service groups. This means that the number of years an employee has worked at Asia Brewery, Inc. does not significantly impact their perception of security policies, knowledge sharing, training adaptation, or overall security management awareness. While there are slight variations in the mean scores across the different years of stay groups, these variations are not statistically significant. Through the Kruskal-Wallis H-test, there was no significant difference in security policies and protocol, knowledge sharing, training adaptation, or awareness among the respondents when grouped according to their years of stay in the company ($p > 0.05$). In simpler terms, employees generally have a consistent level of security awareness, whether they are new or have been with the company for many years. The results support Michalski (2021), arguing that political-administrative factors affect the awareness and practices of security management. Therefore, even after years of service by personnel, conflict still arises, and management resolves it. According to Brown and Green (2020), effective conflict resolution strategies are vital for maintaining security awareness and compliance. Organizations that foster open communication and involve employees in decision-making processes tend to resolve conflicts more efficiently, thereby enhancing overall security awareness.

Table 4.1.1
Test of Significant Difference in the Level of Awareness on Security Management when Grouped According to Years of Stay.

Indicators	Years of Stay	Mean	X^2-Value	p-value	Decision	Conclusion
Security Policies and Protocol	1 to 5	3.59	2.570	0.632	Failed to reject Ho	Not significant
	6 to 10	3.48				
	11 to 15	3.66				
	16 to 20	3.47				
	21 and above	3.6				
Knowledge Sharing	1 to 5	3.68	3.090	0.543	Failed to reject Ho	Not significant
	6 to 10	3.76				
	11 to 15	3.68				
	16 to 20	3.64				

	21 and above	3.4				
Training Adaptation	1 to 5	3.59	2.970	0.563	Failed to reject Ho	Not significant
	6 to 10	3.51				
	11 to 15	3.68				
	16 to 20	3.47				
	21 and above	3.28				
Awareness	1 to 5	3.62	1.750	0.782	Failed to reject Ho	Not significant
	6 to 10	3.58				
	11 to 15	3.67				
	16 to 20	3.53				
	21 and above	3.43				

Legend: Significant if p<0.05

4.1.2 current position

Table 4.1.2 presents a significant difference in the level of awareness of security management when grouped according to the current position at Asia Brewery, Inc. The Mann-Whitney U test demonstrated no significant difference in security policies and protocol, knowledge sharing, training adaptation, and awareness of the respondents when grouped according to their current position in the company ($p > 0.05$). The p-values for all four categories (Security Policies and Protocol, Knowledge Sharing, Training Adaptation, and Overall Awareness) are greater than 0.05 ($p > 0.05$). Therefore, the decision is "Failed to reject Ho" (the null hypothesis), meaning there is no statistically significant difference in the level of awareness between female guards and male guards. This evidence indicates that the current position of the security personnel, whether female guard or male guard, does not significantly impact their perception of security policies, knowledge sharing, training adaptation, or overall security management awareness. While slight differences exist in the mean scores between the female and male guard groups, these variations are not statistically significant. This evidence shows that both groups have similar levels of security management awareness. However, conflict management resolution within organizations, as noted by Lee and Thompson (2022), is inevitable in workplace dynamics. Their research reveals that conflicts related to security management often arise from differing interpretations of security policies among employees and management. A cohesive approach to security management ensures that all employees, irrespective of their tenure, are aligned with the organization's security objectives.

Table 4.1.2
Significant Difference in the Level of Awareness on Security Management when Grouped According to Current Position

Indicators	Current Position	Mean	U-Value	p-value	Decision	Conclusion
Security Policies and Protocol	LG	3.46	466	0.055	Failed to reject Ho	Not significant
	S G	3.59				

Knowledge Sharing	LG	3.71	585	0.432	Failed to reject Ho	Not significant
	S G	3.67				
Training Adaptation	LG	3.46	509	0.132	Failed to reject Ho	Not significant
	S G	3.58				
Awareness	LG	3.55	505	0.127	Failed to reject Ho	Not significant
	S G	3.61				

Legend: Significant if p<0.05; LG-Lady Guard and SG-Security Guard

4.1.3 frequency of training sessions

Table 4.1.3 presents the significant difference in the level of awareness regarding security management when grouped according to the frequency of training sessions at Asia Brewery, Inc. The Kruskal-Wallis H-test displayed no significant difference in security policies and protocol, knowledge sharing, training adaptation, and respondents' awareness when grouped according to the frequency of training sessions in the company (p>0.05). The p-values for all four categories (Security Policies and Protocol, Knowledge Sharing, Training Adaptation, and General Awareness) are greater than 0.05 (p > 0.05). Therefore, the decision is "Failed to reject Ho" (the null hypothesis), indicating that there is no statistically significant difference in the level of awareness across the different training frequency groups. This means that the frequency of training sessions an employee attends does not significantly impact their perception of security policies, knowledge sharing, training adaptation, or overall security management awareness. While there are variations in the mean scores across the different frequency groups (1–5), these variations are not statistically significant. This evidence demonstrates that the security personnel comprehend the provided training information, irrespective of the frequency of their attendance. The findings supported by Jones (2024) explain that security management certification and training are essential to the effective implementation of a security management mission since they guarantee that team members possess current knowledge and abilities. This training could cover auditing, risk assessments, emergency protocols, and regulatory compliance. However, the company mandated certification programs in security management, which have proven to improve the proficiency of security professionals. According to Lee et al. (2023), organizations that prioritize certification attainment among their security personnel tend to demonstrate higher compliance levels with industry regulations and reduced security breaches.

Table 4.1.3
Significant Difference in the Level of Awareness on Security Management when Grouped According to Frequency of Training Session

Indicators	Frequency of Training Session	Mean	X^2-Value	p-value	Decision	Conclusion
Security Policies and Protocol	Once	3.27	8.52	0.074	Failed to reject Ho	Not significant
	Twice	3.60				
	Three	3.69				
	Four	3.54				
	Five	3.62				
	Once	3.43	3.15	0.533		

Knowledge Sharing	Twice	3.8			Failed to reject Ho	Not significant
	Three	3.82				
	Four	3.72				
	Five	3.7				
Training Adaptation	Once	3.33	7.21	0.125	Failed to reject Ho	Not significant
	Twice	3.67				
	Three	3.53				
	Four	3.56				
	Five	3.62				
Awareness	Once	3.34	8.13	0.087	Failed to reject Ho	Not significant
	Twice	3.69				
	Three	3.68				
	Four	3.61				
	Five	3.65				

Legend: Significant if $p<0.05$

4.1.4 educational background

Table 4.1.4 shows the significant difference in the level of awareness about security management when grouped according to educational background at Asia Brewery, Inc. Through the Kruskal-Wallis H-test, there was no significant difference in security policies and protocols, knowledge sharing, training adaptation, or awareness among the respondents when grouped according to their educational background ($p > 0.05$). The p-values for all four categories (Security Policies and Protocol, Knowledge Sharing, Training Adaptation, and Overall Awareness) are greater than 0.05 ($p > 0.05$). Therefore, the decision is "Failed to reject Ho" (the null hypothesis), indicating that there is no statistically significant difference in the level of awareness across the different educational background groups. This means that the educational background of the security personnel does not significantly impact their perception of security policies, knowledge sharing, training adaptation, or overall security management awareness. The findings support Standley System Staff (2024), arguing that security is a team effort; on the other hand, job responsibilities were limited to certain departments. But fewer people may depend on their departments to define their duties, regardless of their education. In addition, interdepartmental collaboration is essential in addressing security challenges. Jones and Taylor (2020) argue that silos within organizations can lead to gaps in security protocols, as departments may overlook potential vulnerabilities that fall outside their immediate responsibilities. By promoting a culture of collaboration, organizations can ensure that all employees are aware of their roles in maintaining security, thereby creating a more robust defense against threats

Table 4.1.4
Significant Difference in the Level of Awareness on Security Management when Grouped According to Educational Background

Indicators	Educational Background	Mean	X^2-Value	p-value	Decision	Conclusion
	CG	3.71	3.552	0.470		

Security Policies and Protocol	G12	3.42			Failed to reject Ho	Not significant
	HS	3.59				
	UG	3.44				
	VC	3.53				
Knowledge Sharing	CG	3.79	1.575	0.813	Failed to reject Ho	Not significant
	G12	3.55				
	HS	3.70				
	UG	3.56				
	VC	3.62				
Training Adaptation	CG	3.66	3.274	0.513	Failed to reject Ho	Not significant
	G12	3.42				
	HS	3.59				
	UG	3.44				
	VC	3.51				
Awareness	CG	3.72	3.311	0.507	Failed to reject Ho	Not significant
	G12	3.46				
	HS	3.63				
	UG	3.48				
	VC	3.56				

Legend: Significant if $p<0.05$; CG-College Graduate, G12-Senior High, HS-High School, UG-Under Graduate and VC-Vocational College

4.2. The level of PRACTICES on security management when grouped according to demographic profile?

4.2.1 Years of stay

Table 4.2.1 presents the significant difference in practices on security management when grouped according to years of stay at Asia Brewery, Inc. The Kruskal-Wallis H-test showed that there was no significant difference in areas like independence in security practices, skill development, team support, and the practices of the respondents based on how long they have worked at the company ($p>0.05$). The p-values for all four categories are greater than 0.05 ($p > 0.05$). Therefore, the decision is "Failed to reject Ho" (the null hypothesis), indicating that there is no statistically significant difference in the perception of security management practices across the different years of service groups. This means that the number of years an employee has worked at Asia Brewery, Inc. does not significantly impact their perception of autonomy, competence, team support, or overall security management practices. The results support Brodowicz (2024), who argues that providing security leadership across their sphere of influence should be the top priority for all managers to contribute to the enterprise's continuation, regardless of years of service. At all times, they ought to promote an atmosphere of collaboration and teamwork. Within their functional area, they ought to give security-related actions the proper direction. Research by Lee et al. (2022) highlights that when security leaders prioritize employee well-being, it leads to increased job satisfaction and organizational commitment. Feeling valued and protected encourages employees to participate actively and share information freely, which is crucial for effective security management.

Table 4.2.1
Significant Difference in Practices on Security Management when Grouped According to Years of Stay

Indicators	Years of Stay	Mean	X^2-Value	p-value	Decision	Conclusion
Autonomy on Security Practices	1 to 5	3.64	5.070	0.280	Failed to reject Ho	Not significant
	6 to 10	3.62				
	11 to 15	3.68				
	16 to 20	3.84				
	21 and above	3.48				
Competence and Skill Development	1 to 5	3.76	3.080	0.545	Failed to reject Ho	Not significant
	6 to 10	3.8				
	11 to 15	3.78				
	16 to 20	3.69				
	21 and above	3.64				
Relatedness and Team Support	1 to 5	3.69	5.310	0.257	Failed to reject Ho	Not significant
	6 to 10	3.6				
	11 to 15	3.51				
	16 to 20	3.62				
	21 and above	3.52				
Practices	1 to 5	3.7	2.910	0.574	Failed to reject Ho	Not significant
	6 to 10	3.67				
	11 to 15	3.66				
	16 to 20	3.72				
	21 and above	3.55				

Legend: Significant if $p<0.05$

4.2.2 current position

Table 4.2.2 shows the significant difference in practices on security management when grouped according to current position at Asia Brewery, Inc. The Mann-Whitney U test showed that there is no important difference in how employees manage security based on their job position in the company, including areas like autonomy, skill development, team support, and overall practices ($p > 0.05$). The p-values for all four categories are greater than 0.05 ($p > 0.05$). Therefore, the decision "Failed to reject Ho" (the null hypothesis) indicates that there is no statistically significant difference in the perception of security management practices between female and male guards. This means that the current position of the security personnel (male guard or female guard) does not significantly impact their perception of autonomy, competence, team support, or overall security management practices. Research indicates that gender-diverse teams leverage a wider range of problem-solving strategies, which is particularly advantageous in unpredictable and complex environments like security operations (Kumar & Zhang, 2020). These teams tend to engage in more comprehensive deliberation, reduce cognitive biases, and foster innovative solutions (Johnson & Miller, 2023). Similarly, Standley System Staff (2024) asserts that security is a collaborative effort, irrespective of gender. However, recently, the distinction between job

duties and responsibilities has blurred. Fewer people may rely on their departments to determine what is and is not part of their duties.

Table 4.2.2
Significant Difference in Practices on Security Management when Grouped According to Current Position

Indicators	Current Position	Mean	U-Value	p-value	Decision	Conclusion
Autonomy on Security Practices	LG	3.64	611	0.606	Failed to reject Ho	Not significant
	SG	3.65				
Competence and Skill Development	LG	3.77	648	0.871	Failed to reject Ho	Not significant
	SG	3.76				
Relatedness and Team Support	LG	3.52	591	0.478	Failed to reject Ho	Not significant
	SG	3.66				
Practices	LG	3.65	612	0.621	Failed to reject Ho	Not significant
	SG	3.69				

Legend: Significant if $p<0.05$, SG-Security Guard, LG-Lady Guard

4.2.3 frequency of training

Table 4.2.3 reveals that the frequency of training sessions at Asia Brewery, Inc. has a mixed impact on the security personnel's perception of security management practices. Specifically, the data shows a meaningful difference in how security personnel view "Autonomy on Security Practices" and "General Practices" depending on how often they receive training, indicated by p-values below 0.05. The evidence suggests that how often employees attend training sessions influences their sense of autonomy and their overall perception of the implemented practices. Notably, those attending training session group 1 consistently report the lowest mean scores, indicating a potentially less favorable perception in these areas. Moreover, the frequency of training does not significantly affect the perceived "Competence and Skill Development" or "Relatedness and Team Support," as the p-values are above 0.05. This conclusion implies that regardless of training frequency, employees maintain a consistent perception of their competence, skill development, and team dynamics. So, while Asia Brewery, Inc. keeps a steady view of skills and team support no matter how often training happens, the company should look into what is taught or how training is given to find out why the number of training sessions impacts feelings of independence and overall practices, especially for those in training session group 1. In summary, the Kruskal-Wallis H-test showed no important difference in how respondents felt about their independence in security practices and their connection with team support based on how often they attended training sessions ($p>0.05$). However, there was a significant difference in their competence and skill development ($x^2=11.47$, $p=0.022$) and overall security management practices ($x^2=10.13$, $p=0.038$) based on training frequency. However, there was a statistically significant difference in the competence and skill development ($x^2=11.47$, $p=0.022$) and overall practices on security management ($x^2=10.13$, $p=0.038$)

when grouped according to frequency of training session. The findings supported by Divyaja (2024) state that security awareness training plays a significant role in the organization's defense strategy. Hence, it is important that the management provide training for the security personnel. In addition, management plays a pivotal role in the implementation and awareness of security practices and training. Alshaikh et al. (2020) assert that this type of training improves the security posture by minimizing human errors, a vulnerability that cybercriminals often exploit. The authors contend that well-trained personnel serve as the primary defense, significantly reducing the risks associated with social engineering, phishing, and other attack vectors. Similarly, Kumar and Singh (2021) highlight that organizations investing in continuous security awareness programs experience a decrease in security incidents. They emphasize that awareness training fosters a security-conscious culture, where employees are more vigilant and proactive in identifying suspicious activities.

Table 4.2.3
Significant Difference in Practices on Security Management when Grouped According to Frequency of Training Session

Indicators	Frequency of Training Session	Mean	X^2-Value	p-value	Decision	Conclusion
Autonomy on Security Practices	Once	3.40	11.47	0.022	Reject Ho	Significant
	Twice	3.73				
	Three	3.69				
	Four	3.50				
	Five	3.73				
Competence and Skill Development	Once	3.61	3.62	0.461	Failed to reject Ho	Not significant
	Twice	3.60				
	Three	3.80				
	Four	3.70				
	Five	3.81				
Relatedness and Team Support	Once	3.57	7.58	0.108	Failed to reject Ho	Not significant
	Twice	3.73				
	Three	3.51				
	Four	3.40				
	Five	3.71				
Practices	Once	3.53	10.13	0.038	Reject Ho	Significant
	Twice	3.69				
	Three	3.67				
	Four	3.53				
	Five	3.75				

Legend: Significant if $p<0.05$

4.2.4 educational background

Table 4.2.4 illustrates the variations in security management practices. Grouped At Asia Brewery, Inc., the Kruskal-Wallis H-test showed that there were no important differences in autonomy on security practices, competence and skill development, relatedness and team support, and practices among the

respondents based on their educational background (p>0.05). The p-values for all four categories are greater than 0.05 (p > 0.05). Therefore, the decision "Failed to reject Ho" (the null hypothesis) indicates that there is no statistically significant difference in the perception of security management practices across the different educational background groups. This means that the educational background of the security personnel does not significantly impact their perception of autonomy, competence, team support, or overall security management practices. The results agree with Sari (2023), emphasizing that modern business practices now emphasize the significance of corporate governance, which highlights the need for efficient oversight and responsibility inside companies. Over time, the dynamics of corporate governance have undergone significant evolution due to a multitude of variables, including globalization, technology breakthroughs, regulatory reforms, and shifting stakeholder expectations, but educational background was not considered. Despite extensive research on the factors influencing corporate governance, the specific role of educational background remains underexplored. While some studies suggest that managerial education impacts governance quality, this variable has not been consistently integrated into the broader discourse (Brennan & Tricker, 2020). Further research is needed to understand how educational qualifications influence governance practices.

Table 4.2.4
Significant Difference in Practices on Security Management when Grouped According to Educational Background

Indicators	Educational Background	Mean	X^2-Value	p-value	Decision	Conclusion
Autonomy on Security Practices	CG	3.75	5.734	0.220	Failed to reject Ho	Not significant
	G12	3.42				
	HS	3.65				
	UG	3.6				
	VC	3.78				
Competence and Skill Development	CG	3.81	0.595	0.964	Failed to reject Ho	Not significant
	G12	3.58				
	HS	3.79				
	UG	3.75				
	VC	3.71				
Relatedness and Team Support	CG	3.61	1.478	0.830	Failed to reject Ho	Not significant
	G12	3.62				
	HS	3.65				
	UG	3.64				
	VC	3.64				
Practices	CG	3.73	0.943	0.918	Failed to reject Ho	Not significant
	G12	3.54				
	HS	3.70				
	UG	3.66				
	VC	3.71				

Legend: Significant if p<0.05; CG-College Graduate, G12- Grade 12 Senior High Graduate, HS- High School Graduate, UG- Under Graduate and VC-Vocational

5. Is there a significant relationship between the level of awareness and practices among security personnel on security management in Asia Brewery, Inc.?

In this table, Table 5 shows the significant relationship between the level of awareness and practices among security personnel on security management in Asia Brewery, Inc**.** Spearman Rho was run to test the significant relationship between the level of awareness and practices among security personnel on security management in Asia Brewery, Inc. The results showed that having freedom in security practices, developing skills, support from the team, and overall practices were strongly connected to security policies and protocols, sharing knowledge, adapting training, and overall awareness ($p<0.001$). All p-values are less than 0.001 ($p < 0.001$), which is significantly less than 0.05. Therefore, the decision is "Reject Ho" (the null hypothesis) for all relationships, indicating statistically significant relationships. The positive Rho values across all variables indicates a positive correlation. This means that as the level of awareness increases, the perceived positive practices of security management also increase, and vice versa. The very low p-values ($p < 0.001$) indicate a very high level of confidence in the significance of these relationships. In simpler terms, there is a strong link between how well the security personnel understand the security information and how well they put the security practices into action. The findings delved into the cognitive aspects, revealing that when personnel understand the rationale behind security procedures, they are more motivated to adhere to them diligently. Kang and Lee (2021) demonstrated that security personnel with a deeper understanding of threat vectors and mitigation strategies were more proactive in applying security measures and reducing vulnerabilities. Zhang and Zhao's (2021) research further supports the interconnection between security management and operational performance. They found that effective security practices not only mitigate risks but also streamline operational processes. This dual benefit contributes to improved performance outcomes, as firms can operate more efficiently and respond to market demands promptly.

Table 5

Test of Significant Relationship between the Level of Awareness and Practices Among Security Personnel on Security Management in Asia Brewery, Inc.

Indicators	Rho	p-value	Decision	Conclusion
Autonomy on Security Practices				
Security Policies and Protocol	0.624	< .001	Reject Ho	Significant
Knowledge Sharing	0.593	< .001	Reject Ho	Significant
Training Adaptation	0.659	< .001	Reject Ho	Significant
Awareness	0.690	< .001	Reject Ho	Significant
Competence and Skill Development				
Security Policies and Protocol	0.507	< .001	Reject Ho	Significant
Knowledge Sharing	0.581	< .001	Reject Ho	Significant
Training Adaptation	0.552	< .001	Reject Ho	Significant
Awareness	0.591	< .001	Reject Ho	Significant
Relatedness and Team Support				

Security Policies and Protocol	0.618	< .001	Reject Ho	Significant
Knowledge Sharing	0.638	< .001	Reject Ho	Significant
Training Adaptation	0.621	< .001	Reject Ho	Significant
Awareness	0.685	< .001	Reject Ho	Significant
Practices				
Security Policies and Protocol	0.705	< .001	Reject Ho	Significant
Knowledge Sharing	0.714	< .001	Reject Ho	Significant
Training Adaptation	0.732	< .001	Reject Ho	Significant
Awareness	0.789	< .001	Reject Ho	Significant

Legend: Significant if $p<0.05$

6. Based on the findings, what action plan can be proposed to enhance respondents' awareness of and practices regarding security management?

6.1. Proposed Action Plan

Key Result Areas	Goals	Strategies	Activities	Lead Person	Time Frame	Estimated Budget	Expected outcome
I-Reinforce Training & Development	Corporate Security Supervisor must undergo Certified Security Professional (CSP) Training, Advanced Security Management (ASM) Course 1, 2 & 3, Certified Security Investigator (CSI), and Fire Safety Officer Training	1. Develop investigative skills and fire safety awareness. 2. Provide foundational and advanced knowledge in occupational safety. 3. Equipped with advanced knowledge in security management, occupational and safety training, including threat analysis and	1. Case studies, simulations, and practical exercises on security planning. 2. Assess to mitigate risk and other safety protocols 3. Properly handle sensitive cases for investigation	Corporate Security Supervisors	Typically, estimated a total of 6 months with 180 learning hours (gradually based on ABI security management program)	The catering training center will define the total fees and expenses. However, it is funded by the corporate security of Asia Brewery, Inc.	The Corporate security supervisor should be able to implement security policies, manage security teams, and conduct risk assessments effectively.

	(FSOTC) Course, and Basic and Advanced Safety Officer Course (BOSHC and OSH)	emergency response.					
	Suggest that all supervisory positions must undergo Certified Security Professional (CSP) Training, Basic and Advanced Officer Safety & Health Course Training (BOSH)	1. Enhance risk awareness and hazard prevention 2. Boost Operational Performance 3. Promote a Safety-Oriented Culture	Properly improve a safer work environment, and properly implement the company policy and procedure.	Detachment Commander, Shift-in-charge, and Head guards	40 Hours or 1 week Training	CSP and BOSHC Training fees are provided by an accredited training center the total cost and funded by the security agency	Improve Incident Response and Emergency Readiness, boost their morale, and higher productivity
	Security personnel with knowledge in computers and/or willing to train are suggested to undergo safety and	1. Can mitigate risk, identify hazards, implement safety protocols, and ensure regulatory compliance.	1. Provide hands-on training on CPR, wound treatment, fire response, and evacuation.	Security personnel with knowledge of computers and willing to learn.	1. Based on the Phil. Red Cross standard time frame 2. It's a 12-hour internal	1. First Aid Training is free and provided by corporate security management.	Stronger safety culture and preparedness among frontline personnel.

	first aid training, and CCTV Operator.		2. Train CCTV operators on how to monitor for safety violations and spot early warning signs of emergencies.		CCTV Training session on weekends.	2. CCTV Operator free training	

Key Result Areas	Goals	Strategies	Activities	Lead Person	Time Frame	Estimated Budget	Expected outcome
II. Strengthen Knowledge Sharing	1. Encourage all senior or veteran security personnel and newly recruited security personnel must share their knowledge during formation or guard mounting.	1. Mentorship Program 2. Knowledge Exchange Discussion 3. Feedback Loop	1. Improved information dissemination and collaborative problem-solving. 2. Increased knowledge contribution and a collaborative environment.	Corporate Security Supervisor, Senior Security Personnel, DC, SIC, and newly hired security guards	During formation, daily tour of duty, and even in the flat forms like Facebook Messenger.	Not applicable Personal aspect	1. Contribute to a more efficient and cohesive workforce ready to navigate dynamic workplace demands 2. Develop self-confidence and strong decision-making, and a richer pool of knowledge within the organization

III. Enhance Team Dynamics & Support	1. Create an Anonymous Feedback Box 2. Team Sports or Fitness Challenges	1. Conducted regular review process by encouraging to write feedback in an anonymous letter or submit through platforms by direct message (DM) the admin in the FB messenger group chat (GC). 2. Fostering team building, camaraderie, and collaboration	1. Place a box in common areas or create a digital version for convenience. 2. Basketball, volleyball, or running groups.	Corporate Security Supervisor, DC, SIC, Security Personnel, and a representative from the Security Agency	Conducted every quarterly	Not applicable	1. Employees feel heard and valued. Security personnel recognize leadership's commitment to improvement. 2. Boost collaboration and morale.
IV. Consistent Implementation & Evaluation	Conducted monthly rank inspection.	Ensure all compliant paraphernalia is clean and complete	Conducted for all security personnel during the incoming and outgoing formation.	Corporate Security Supervisor, DC, SIC	1-hour session	Not applicable	All security personnel must adhere to company policy and standards.
V. Data-Driven Approach	1. Conducted security personnel Productivity Metrics 2. Monitor the effectiveness of the action plan.	1. Conducted quarterly performance assessment. 2. Establish Key Performance Indicators (KPI) to measure the impact of action plans.	1. Measurable improvement in security awareness and practices. 2. Discuss and give a stern warning to those with unsatisfactory	Corporate Security Supervisor, DC, SIC, and Representative from Security Agency	Weekly, Monthly, Quarterly, Semi-Annual, and Yearly	Not applicable	Develop honest and trusted security personnel in an efficient security framework for safeguarding company assets and

			performance.				the safety of stakeholders.

5. CONCLUSIONS

The study reached the following conclusions based on its findings:

1. The majority of the respondents have been working in the organization for 1–5 years, most of them are male security guards, they have been attending training five times a year, and are high school graduates. However, those who have graduated with their respective bachelor's degrees and professions are absorbed into the company.

2. The respondents are very much aware of the security policies and protocols, knowledge and sharing, and training adaptation, which indicates that the organization's efforts in communicating and implementing security policies, facilitating knowledge sharing, and providing effective training are generally successful. The respondents consistently apply all parts of security management, independence in security actions, skill improvement, and teamwork support, showing a strong and steady positive view of security management practices in all three areas among security staff.

3. There is no significant difference in the level of awareness of the respondents on security management when grouped according to the years of stay in the company. Similarly, there is no significant difference that exists when grouped according to their current position in the company; the same goes for the training sessions attended and educational background. Furthermore, there is no significant difference in the respondents' practices in security management when grouped according to years of service and current position in all components. Similarly, no significant difference was found in the areas of competence and skill development and in relatedness and team support when grouped according to training sessions attended. On the other hand, a significant relationship was found in the areas of autonomy, security practices, and protocol, which means that how often employees attend training sessions influences their sense of autonomy and their overall perception of the practices implemented. Furthermore, we found no significant difference in terms of educational background.

4. The findings reveal that there is a significant relationship between the respondents' level of awareness and security management practices. This means that as the level of awareness increases, the perceived positive practices of security management also increase, and vice versa.

5. The findings lead to the conclusion that awareness significantly influences security practices. Rejecting the null hypothesis across all variables confirms that greater understanding of security protocols translates to improved execution of security measures. Personnel who have a deeper grasp of security principles are more likely to apply them effectively, contributing to a more secure and efficient operational environment.

6. The action plan presented by the researcher serves as a structured roadmap for strengthening security measures and strategic framework of security personnel and management. To ensure the protection of personnel, assets, and operational integrity. Likewise, to strengthening their security

awareness and practices in implementing standards and protocols of the company. Nevertheless, this action plan reinforces a culture of proactive security and builds security conscious workforce that capable for preventing and responding to threats effectively and efficiently.

6. ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to Dr. Lani D. Deada, my adviser, and Dr. Remedios Bucal, our subject professor in the Thesis Writing Seminar, respectively. Their guidance, support, and encouragement were invaluable throughout this research. Your expertise and insights have significantly contributed to the success of this study.
I am also profoundly grateful to Dr. Urbina, Dr. Unico, and Dr. Pendon, whose constructive feedback and advice helped shape the direction and quality of this research. Also, my heartfelt thanks go to my previous professors, colleagues, and friends: David, Ray, Maricar, Celica, Kag. May, Lino, Rhaf, and others, for their continuous support, insightful discussions, and encouragement during the challenging phases of this project. Your camaraderie and motivation were greatly appreciated. To my Boss and Mentor, GEN NOEL A. COBALLES, AVP-Corporate Security of Asia Brewery, Inc., thank you for granting me permission for my thesis. Likewise, I thank my boss, Alben Carbonera, and Doc Rommel Maulanin for sharing their ideas and knowledge to make this possible. To the agency deployed in Asia Brewery, Inc., and to my subordinates, security personnel who participated in this study. Your openness and willingness to share your experiences and insights were crucial for the completion of this research.
A special thanks to my family for their unwavering support, patience, and understanding. Your belief in me has been a constant source of strength.
Lastly, I am grateful to everyone who, in their own way, contributed to the successful completion of this research. Thank you all for your support and encouragement.
Above all, thanks to God for the wisdom and blessing received from Him all the time.

REFERENCES

1. Alhassan, I., Kankam, H., & Yeboa, E. (2020). "Security Management Awareness in Developing Countries: A Comparative Study." Journal of Security Studies, 12(3), 45-62.
2. AlHogail, A. (2020). Design and Implementation of Security Policies in Cloud Computing. Journal of Cybersecurity, 6(2), 45-59.
3. Alqahtani, F., Kavakli-Thorne, M., & Alharthi, M. (2022). "Security Awareness and Training Programs: A Review." Journal of Information Security and Applications, 66, 103146.
4. Al-Mawali, H., Al-Debei, M. M., & Tarhini, A. (2022). Empowering front-line employees in security and risk-based decision-making. Journal of Risk Research, 25(2), 240–256.
5. Alshaikh, M. (2020). "Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective." Computers & Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003
6. Alshaikh, M., Alzain, M. A., & Alzain, L. (2020). Enhancing organizational security through employee awareness training: A systematic review. Journal of Cybersecurity and Information Management, 8(2), 45-59.
7. Asia Brewery, Inc. (2023). Annual Report.
8. Bari, M. W., Fanchen, M., & Ullah, M. (2021). Employee empowerment and job satisfaction: The mediating role of psychological ownership. Frontiers in Psychology, 12, 621875.

9. Bautista, R. (2020). Enhancing Security Personnel Performance through Training and Development in Manufacturing Plants. Philippine Journal of Security Studies, 15(2), 45–59.
10. BeesyPapers. (2023, June 22). Security Management as Integral Part of Organization. https://beesypapers.com/security- management-as-integral-part-of-organization/
11. Brennan, N., & Tricker, R. (2020). Corporate Governance: Principles, Policies, and Practices. Oxford University Press.
12. Brodowics, A. (2024). Security Management in the Age of Digital Transformation. Security Management Review, 28(1), 34-49.
13. Brodowicz, M. (2024). The priority of security leadership in organizational sustainability. Journal of Enterprise Security, 7(2), 1-15.
14. Brown, T. & Green, A. (2020). "Conflict Resolution in Security Management: Strategies for Success." International Journal of Security Studies, 15(2), 112-130.
15. Burge, S. (2023, April 1). What is Industrial Security Management? International Security Journal. https://internationalsecurityjournal.com/industrial-security-management/
16. Chen, Y., Liu, X., & Wang, Z. (2021). Effective dissemination of security policies in large-scale organizations. Journal of Cybersecurity, 7(2), 45-58.
17. Cybersafe. (2023). Security awareness training: Recognize, identify, prevent. Cybersafe Publications.
18. Decuypere, A., & Schaufeli, W. (2020). Leadership and work engagement: Exploring explanatory mechanisms. Journal of Leadership & Organizational Studies, 27(3), 237–250.
19. Deci, E. L., & Ryan, R. M. (1985). Intrinsic motivation and self-determination in human behavior. Springer Science & Business Media.
20. Dela Cruz, J., Ramos, P., & Uy, M. (2021). Technological Integration in Industrial Security: The Philippine Experience. Asian Security Review, 8(1), 33–49.
21. Divyaja. (2024, February 15). Security Awareness Training and it's Importance - 2024 - PhishGrid. PhishGrid https://phishgrid.com/blog/security awareness-training/
22. Divyaja, S. (2024). Security Awareness Training's Role in Organizational Defense Strategy. Journal of Cybersecurity Research, 12(4), 245-260.
23. Domas, S. (2023) Security Autonomy Is Coming—What Is It, And Is It Good For Security?https://www.forbes.com/councils/forbestechcouncil/2023/01/03/security- autonomy.
24. Faster Capital (2024) Policy enforcement: The Backbone of Effective Regulation. (n.d.)., from https://fastercapital.com/content/Policy-enforcement--The-Backbone-of-Effective-Regulation.html
25. Fuentes, L., & Almonte, R. (2021). Indicators of Security Policies and Procedures among Stakeholders of Laguna Polytechnic University. Philippine Journal of Higher Education, 22(3), 101-115.
26. Garcia, A. & Yu, S. (2021). Private Security Challenges in Southeast Asia's Beverage Industry. Asia-Pacific Security Management Journal, 12(4), 102–118.
27. Garcia, L. (2022). Advances in Security Technologies and the Need for Continuous Training. Security Journal, 35(4), 245-260.
28. Geldenhuys, M., Laba, K., & Venter, C. M. (2020). Meaningful work, work engagement and organisational commitment. SA Journal of Industrial Psychology, 46(1), 1–10.
29. Grimmick, R. (2023) What is a Security Policy? Definition, Elements, and Examples. https://www.varonis.com/blog/what-is-a-security-policy#definition

30. Guthrie, G. (2024). How to create a knowledge-sharing culture (a step-by-step guide). https://nulab.com/learn/collaboration/knowledge-sharing/
31. Henriquez, L. (2022). The impact of security program stagnation on business protection. Security Management Review, 18(4), 45-59.
32. Henriquez, M. (2022, April 28). Strategies for supporting security teams. Security Magazine. https://www.securitymagazine.com/articles/97511-strategies-for- supporting-security-teams.
33. Hengstler, J., Smith, L., & Lee, R. (2022). Social interactions and deviant behavior: A social cognitive approach. Journal of Social Psychology, 162(3), 245-262.
34. International Association for Security Management (IASM). (2022). "Global Security Awareness Survey Report." Retrieved from IASM.
35. International Labour Organization (ILO). (2020). Skills shortages and labor market challenges in the Philippines.
36. International Labour Organization (ILO). (2020). Women in Private Security Services. Geneva: ILO Publications.
37. Jeanpert, S., Jacquemier-Paquin, L., & Claye-Puaux, S. (2021). The role of human interaction in complaint handling. Journal of Retailing and Consumer Services, 62, 102670. https://doi.org/10.1016/j.jretconser.2021.102670.
38. Johnson, P. (2020). Awareness versus instruction: Clarifying their roles in security education. International Journal of Information Security, 18(4), 321-330.
39. Johnson, P., & Miller, R. (2023). Cognitive diversity and decision-making under pressure: Evidence from high-stakes environments. International Journal of Organizational Behavior, 29(4), 567-583.
40. Johnson, R., Smith, A., & Lee, K. (2021). The role of random sampling in social research: Ensuring representativeness. International Journal of Quantitative Research, 10(1), 45–59.
41. Johnson, R. (2024). Continuous Learning in Security Management: A Necessity for Success. Security Management Review, 12(1), 23-34.
42. Jones, P., & Taylor, S. (2020). The Impact of Organizational Silos on Security Protocols. Journal of Organizational Security, 15(4), 210-225.
43. Kang, S., & Lee, J. (2021). Cognitive Factors and Security Practice Compliance among Security Personnel. Journal of Security Studies, 45(2), 123-138.
44. Kim, H., & Park, S. (2023). Cultivating competence through skill development programs and its effect on employee intrinsic motivation. Journal of Organizational Psychology, 45(2), 123-138.
45. Klein, H. J., & Molloy, J. C. (2020). The role of employee turnover in the performance of organizations. Journal of Applied Psychology, 105(4), 387-400.
46. Kraus, S., Clauss, T., Breier, M., Gast, J., Zardini, A., & Tiberius, V. (2020). "The economics of COVID-19: initial empirical evidence on how family firms in five European countries cope with the corona crisis." International Journal of Entrepreneurial Behavior & Research, 26(5), 1067-1092.
47. Kumar, S., & Zhang, Y. (2020). Gender diversity and problem-solving in security operations: A comparative analysis. Security Journal, 33(1), 45-60.
48. Kumar, S., & Zhang, Y. (2020). Gender diversity and problem-solving effectiveness in complex environments. International Journal of Management Studies, 27(2), 110-125.
49. Kumar, S., & Singh, R. (2021). Impact of continuous security awareness programs on organizational security posture. Journal of Information Security, 14(4), 234-249.

50. Lee, C., & Thompson, H. (2022). Conflict Management in Security Protocols: Aligning Employee and Management Perspectives. International Journal of Security Management, 15(1), 78-92.
51. Lee, H., Kim, S., Park, J., & Choi, Y. (2023). Certification attainment and security performance: Evidence from organizational practices. International Journal of Security Management, 17(2), 89-105.
52. Lee, H., & Kim, S. (2020). Collective Intelligence in Security Teams: The Role of Knowledge Sharing. International Journal of Security Studies, 12(3), 89-105.
53. Lee, H., & Tan, J. (2022). Leadership Styles and Security Management Effectiveness in Southeast Asian Manufacturing Firms. International Journal of Industrial Security, 7(2), 70–85.
54. Lopez, A., & Tan, S. (2021). The rise of competency-based hiring in the Philippine labor market. Asian Journal of Employment Studies, 4(1), 55-70.
55. Michalski, Krzysztof. (2021). INCREASING COMPLEXITY OF TECHNICAL SYSTEMS - NEW CHALLENGES FOR SECURITY MANAGEMENT. 10.26410/SF_4_2/21/6.
56. Michalski, R. (2021). The influence of political-administrative factors on security management awareness and practices. Journal of Security Studies, 45(2), 123-139.
57. Miller, J., & Roberts, T. (2020). Creating a proactive security culture: Measures and best practices. Cybersecurity Perspectives, 12(3), 10-20.
58. Mimecast. (n.d.). What is Security Awareness Training? Mimecast. https://www.mimecast.com/content/what-is-security-awareness-training/
59. NIST. (2023). "Framework for Improving Critical Infrastructure Cybersecurity." Retrieved from NIST.
60. Nguyen, T. T., Tran, Q. H., & Pham, T. H. (2022). Trust and Agility in Organizational Decision-Making. Management Science, 68(1), 45-60.
61. Park, S., Newman, A., Zhang, L., Wu, C., & Hooke, A. (2020). Mentoring and knowledge sharing in the workplace: The role of perceived organizational support. Journal of Business Research, 115, 125–136.
62. Philippine National Police Supervisory Office for Security and Investigation Agencies (PNP-SOSIA). (2022). Annual Report on Security Personnel Statistics.
63. PowerDMS (2020) Why Are Policies and Procedures Important in the Workplace. https://www.powerdms.com/policy-learning-center/following-policies-and-procedures-and-why-its-important
64. Santos, K., & Lim, E. (2022). Digital Security Infrastructure in Philippine Manufacturing: A Case Study of Asia Brewery, Inc. Journal of Corporate Security, 9(3), 21–36.
65. Sari, Ratna. (2023). Enhancing Corporate Governance through Effective Oversight and Accountability. Advances: Jurnal Ekonomi & Bisnis. 1. 10.60079/ajeb. v1i6.291.
66. Smith, J., & Brooks, A. (2020). Managing security risks: Understanding threat interactions at multiple levels. Security Studies Review, 8(3), 112-128.
67. Smith, J. (2020). The Role of Security Guards in Modern Security Operations. Security Management Journal, 45(2), 112-119.
68. Smith, J., et al. (2021). Continuous Training and Security Readiness: Evidence from the Field. Security Administration Journal, 19(2), 59-72.
69. Smith, R., Brown, T., & Patel, A. (2020). The role of feedback in technical skill acquisition. Skills Development Journal, 15(2), 78–89.

70. Standley Systems Staff (2024). Security Is a Team Effort. https://www.standleys.com/blog/security-is-a-team-effort.
71. Standley System Staff. (2024). [Title of the publication or report]. Unpublished manuscript.
72. Standley System Staff. (2024). Security as a Collaborative Effort: An Inclusive Approach. Internal Report.
73. Smith, A., & Jones, B. (2021). "Categorizing Security Management Practices: A Comprehensive Review." Security Management Journal, 10(1), 5-20.
74. Smith, D., & Lee, H. (2021). Job Satisfaction and Tenure among Security Guards. Employee Relations Today, 47(2), 58–70.
75. Tulane University Security Report. (2023). Tulane University. Retrieved from https://tulane.edu/security-report
76. U.S. Bureau of Labor Statistics. (2023). Employee Tenure Summary. Retrieved from https://www.bls.gov/news.release/tenure.nr0.htm
77. Verizon. (2023). "Data Breach Investigations Report." Retrieved from Verizon.
78. Villanueva, C. (2023). Fostering a Proactive Security Culture: Lessons from Asia Brewery, Inc. Business Security Insights, 4(2), 58–67.
79. Wibowo, A., Ma'arif, M. A., & Darmawan, D. (2021). Effect of feedback on employee skill development in security operations. Journal of Security and Strategy Studies, 3(2), 34–44.
80. Wu, C., Parker, S. K., & de Jong, J. P. (2021). Need satisfaction at work and proactive behavior: The role of autonomy and competence. Journal of Management, 47(4), 955–983.
81. Zammani, M., Razali, R. and Singh, D., 2021. Organizational Information Security Management Maturity Model. International Journal of Advanced Computer Science and Applications, 12(9).
82. Zhang, L., & Zhao, X. (2021). "Linking Security Management to Operational Performance in the Maritime Sector." Journal of Shipping and Trade, 6(2), 1-15.
83. Zhang, Y., Li, X., & Wang, J. (2020). Enhancing security personnel motivation through management support and autonomy. Security Management Journal, 14(3), 45–59