BEST WESTERN PLUS ATLANTIC

HOTEL

TAKORADI, GHANA

INFORMATION TECHNOLOGY SYSTEMS AUDIT REPORT 2024

Audit Lead: Samuel Melchizedek Osei

SEPTEMBER 2023-24

TABLE OF CONTENT

1.0 OVERVIEW

1.1 EXECUTIVE SUMMARY

The audit team of Best Western Atlantic Hotel assessed the efficiency and productivity of our information technology system controls with major focus on access control, password management policy, application and network control, data privacy etc.

The audit is to evaluate the company's IT infrastructure, software, applications and IT policies to ensure alignment with industry best practices and regulatory requirements internationally.

1.2 AUDIT OBJECTIVES

The aim of this audit is to evaluate and assess the operationalization and efficiency of IT system controls at Best Western Atlantic Hotel to ensure best practices to safeguard customers data while using their services and also whether their IT policies align with international regulatory requirement.

1.3 AUDIT SCOPE

The scope of the audit is to assess the efficiency of IT system controls used by Best Western Atlantic Hotel. It details a comprehensive audit on the effectiveness of company's policies, access controls, compliance with international standards and regulations and necessary recommendations to safeguard the IT environment.

1.4 INTRODUCTION

Best Western Atlantic Hotel is a highly rated 5-star hotel that serve approximately 200,000 customers annually. The company handles and process sensitive data, customers and key stakeholders rightly expect the company to protect their information including Personal Identified Information (PII), E-transaction details (payment card: VISA, MATERCARD, DISCOVER etc.), security and access control. In this audit, we focused on whether all forms of sensitive data were completely and accurately obtained, processed and maintained to ensure confidentiality, integrity, data privacy, availability and security. The audit reviewed five (5) key control findings/parameters and each is important to the operations of Best Western Atlantic Hotel. The audit was actually carried on this control parameters:

- Password management control.
- Application and network control.
- Electronic payment system control (Payment Card Industry)
- Data privacy and backup control.
- Business continuity and risk management control.

2.0 AUDIT FINDINGS AND RECOMMENDATION

The audit kickstart by scheduling meetings with system owners to test the operational effectiveness of the controls. The process involves examination, interview and testing of the controls.

2.1 Access control (Password management)

Audit finding:

Best western Atlantic hotel IT system have diverse range of users including employees (staff), management, customers, partners (third party contractors). These require different types of accounts or identities to access information from inside and outside the company. For example:

- Employees: Normal user accounts for staff to perform day-to-day tasks
- Partners: contractors and vendor support staff
- Privilege Accounts: Individuals with high level administrative privileges such as system, network and database administrator
- Customer: high profile customers have account based on business need to know.

Password remain the main control the company use to protect its data and security mechanism. The company has password policy with the following parameters:

- Password must have 12 characters with at least an uppercase, lowercase and special character.
- Password must not include guessable name or dictionary word.

We collected and gathered around two hundred passwords from diverse users for the audit. It was realized that passwords of most users are weak passwords for both onsite and offsite login. Though the password were 12 characters in length, it was not adequately secured. Notable exception in the password seen were:

- **names of users, birthdate of users, povidone's name, meme names and other guessable names etc.**

.

- Examples: **Godfirst1234, Security1000, manager111111, Appiah1990, Humblelion1234, Bestwesternhotel123** etc.

Risk impact

Weak password exposes the company system to vulnerabilities. Bad actors use brute force attack, phishing email to exploit these vulnerabilities to cause harm and damages to the company including data breaches, credential theft and ransomware.

Root cause analysis

Though the company has password management policy, it was not actually enforced. No access request form (ARF) was issued to staff to fill and submit before granting access. The parameter in password formulation was not completely adhered.

Recommendation

The security and access control department should:

- Enforce the password management policy with stringent measures for everyone including defaulters to ensure every password meet the password requirement.
- Ensure there is a password change every six monthly to strengthen the security standard and avoid cyberattack especially brute force attack.
- Undertake a routine security and awareness training for the entire staff including third party vendor to ensure challenges are addressed and melted out.
- Ensure multifactor authentication are used for remote access to the system.
- Implement a guideline on privilege access to avoid access abuse and vulnerabilities.

2.2 Application and network control

Audit finding

The database and network administrators walk us through the applications and network systems deployed in the company. The application includes enterprise resource planning software (ERP), oracle database etc. The network infrastructure includes internet connectivity system/server(routers), CCTV, computers/desktops and managed service providers (MSP). The following were observed by the audit team:

- Frequent change of enterprise resource planning software within a year (three times in the year 2023)
- Staff are not well trained on most of the software causing less utilization of the software and affecting productivity.
- Internet servers do not have password therefore can be accessed randomly by anyone.
- Activities of MSP are not properly monitored and regulated.
- Audit trail is not effectively implemented to check system logins and application usage.
- The company do not have clear policy on RTO and RPO to ensure efficient data backup and recovery.
- Outdated SSL or TLS on the webpage.

Risk impact

Vulnerabilities in the application and network infrastructure was a great concern as it can lead to data and credential theft, data breaches, man-in-the-middle attacks, IP address leakage and possibly

distributed denial of service (DDOS) on company server. The company reputation and brand can be damaged with potential fine when attackers exploit these vulnerabilities.

Root cause analysis

The root cause includes regular change of software especially ERP, no change management policy, lack of segregation of duties. There was also 1lack of security and awareness training for staff therefore they have challenges utilizing certain software. Management do not solicit technical advices from application and network administrators when sourcing or procuring software and network gadgets.

Recommendation

- Management should a comprehensive and efficient enterprise resource planning software for the company for specific years before any changes.
- Management should regularly consult application and network administrators on key decisions regarding software, network gadget and other essential gadgets purchase.
- Network and internet servers should have password or authenticator before granting access to anyone.
- Audit trail should be implemented on the premise to track application and network access for swift actions when necessary.
- Company webpage should be secured with current TLS version to ensure secure and seamless access on the webpage.
- Activities of third-party vendors including MSP should be properly regulated and ensure compliance with international standard.

2.3 Payment card industry (Electronic payment system)

Audit finding

Best western Atlantic hotel accept payment of service through various medium of transaction. One of the medium of transaction is payment cards predominantly VISA, MASTERCARD, AMERICAN EXPRESS. The account office handle transactions through payment cards. These cards are used by customers predominantly foreign nationals to transact business at the premise of the company. There are also Mobile merchant numbers from local telecom networks especially MoMo-Pay (MTN), VodaCash (Telecel), TigoCash (Airtel-Tigo) for customers who wants to transact service on local service providers. This transaction is used predominantly by the local customers. Through the audit process, this finding was highlighted:

- There was no designated personnels or team with knowledge and experience on payment card industry data security standard (PCI DSS) in charge to handle it.

- There is no proper policy and framework on payment card industry to ensure stringent compliance with payment card industry security standard council (PCI SSC).
- There is no contract of merchant and credit service providers (MSP & CSP) to handle technical issues when a customer has challenge doing transaction with payment card.
- There was no merchant compliance requirement, that is self-assessment questionnaire (SAQ), approved scan vendor report (ASV report) indicating PCI DSS compliance.

Risk impact

No compliance to PCI DSS requirement is a great threat to the company's brand, finances and marketability. PCI is very critical when payment of service is rendered through e-transaction. Any potential investors will withdraw their money when there is no document to show PCI DSS compliance. Defaulters are heavily fined, to sum of millions of dollars and potentially shortlisted in the MATCH list (member alert to control high risk merchant).

Root cause analysis

Through the audit we observed that the account office handles transactions with payment cards. None of these staff at the account office have knowledge and experience on PCI DSS environment. With this, the company was vulnerable to all forms of attacks involving transaction of money through payment cards which could have led to heavy penalty or fine when defaulted.

Recommendation

- Management should recruit personnel who is competent and experienced on PCI DSS environment.
- Management should collaborate with experienced PCI DSS officer to ensure compliance with PCI DSS requirement.
- Regular self-assessment questionnaire, approved scan vendor report on the merchant level to strengthen customers confidence.
- Readily availability of SAQ, ASV report to potential investor and partners to boost their confidence and trust in the transaction activities of the company.

2.4 Data Privacy and backup control

Audit finding:

Data privacy involves the practices that ensure data is handled, stored, and transmitted securely and in accordance with frameworks and regulations. Data Backup is a mechanism whereby data is continuously updated/backed up on a storage media to avoid data loss during disruption. Data privacy has key principles on which it works. These key principles of data privacy are transparency, consent, retention and minimization. An audit was conducted on data privacy and backup procedure of the

company especially customer's Protected Identifiable information (PII), PCI transactions and other sensitive data. The following exceptions were noted and require management attention:

- No advanced encryption algorithm (AES 124) to encrypt various forms of data at rest, motion or transit.
- No regular awareness training on data privacy and backup for employees to sharpen their understanding on the importance of data privacy and backup procedures.
- There was no asymmetric encryption on data in transit or motion so it is more vulnerable to cyberattacks.
- Abuse of Least privilege access by system administrators, management etc.
- Lack of audit trail to monitor the details of staffs that access data on the system.
- There was no RTO and RPO plan on data storage and backup in case of disruption.
- No offsite storage media to store data and retrieved in case of disruption on the systems.

Risk impact

Cyberattacks on company data especially highly sensitive data and personal identified information of customers and staff is a grave concern to every organization. The company can be sued for data breaches, phishing attacks. The company could lose its credibility, marketability and brand as well as customers when data privacy is compromised.

Root cause analysis

During the audit, we observed that there is no policy on data privacy. Most of the staff have little or no knowledge on data privacy. There was no awareness training on data privacy for staff since the company inception. For backup, there was no guidelines on RTO and RPO plan so it was done only on the company database without dedicated offsite storage media.

Recommendation

- Awareness training on data privacy should be conducted every half of the year,
- A policy on data privacy should be enacted to act as guideline on data management and access.
- Least privilege access should operate on business need-to-know basis.
- Regular assessment on the database to assess vulnerabilities and possibly patch it.

2.5 Business continuity and risk management plan

Audit finding

Business continuity control is a robust plan that outline procedures and guidelines to ensure sustainability of the business function during disruptions such as cyberattack, natural disasters etc.

Risk management on the other hand is the procedures and strategies harnessed to mitigation risk and any vulnerabilities in the company. Business continuity and risk management have a strong synergy and these two are critical to the success and achievement of Best Western Atlantic hotel. Business continuity plan when fully implemented can benefit the organization in diverse ways including, it increases customer's confidence, compliance with regulatory organization and enhances resilience and adaptability of staff. An audit was conducted on the business continuity and risk management control of the company. The following were the exceptions noted:

- There was no business impact analysis to assess the impact of disruptions on business operation.
- No communication plan regarding risk management and business continuity.
- No awareness training and workshop on business continuity and risk management policy.
- There was no comprehensive policy or control on business continuity and risk management.
- No RTO and RPO to ensure sustainability of business operations during disruption.

Risk impact

The impact of a failed business continuity control and risk management is enormous and can severe consequences on the business operation of the company. It can lead to revenue loss, data loss, loss of customer trust and possibly regulatory penalties. The brand and marketability of the company can be damaged.

Recommendation

Management should act on these few recommendations to address the exceptions noted during our audit on business continuity and risk management control.

- Implement robust risk management policy to address and mitigate potential threat, attacks and vulnerabilities.
- Implement efficient business continuity plan for the company to handle any unforeseen disruptions to ensure business operation is running.
- Frequent awareness training on risk management and business continuity to all staffs.
- Hire a certified risk management officer or vulnerability officer to regularly check the system and update management on potential vulnerabilities and threats in the company.
- Regularly conduct vulnerability test on the IT systems and patch it appropriately.
- Distribute BCP and RMP to all key stakeholders.

3. CONCLUSION

This internal audit was successfully completed on 18th September 2024 under the supervision of chief information officer. It was carried on five significant controls and the exception noted has been highlighted in the report. The government of Ghana acknowledge cyberattacks, system vulnerabilities as one of the threats to national security and Best western Atlantic hotel is committed to developing a robust cybersecurity strategy to support its operation and future requirement. There are robust recommendations on each system/control audit and management have been notified. They have tasked the system owners to execute the recommendations to effectively mitigate the threats, vulnerabilities in the system. Best western Atlantic hotel is excited to inform well valued stakeholders that, there is no data and financial breaches, international regulatory requirement discrepancies/shortfalls during the audit but the audit is critical for business function of the company.

Dr. Noah Darko-Adjei	Samuel M. Osei
Chief information officer	Audit team lead
……	……

4. REFERENCES

Nist 800-53 v5
PCI DSS (Payment Card Industry Data Security Standard)
ISO 27001 (International Standard Organization)
GDPR (General Data Protection Regulation)