Cybersecurity Audit Report

Northside Coffee

Introduction

Northside Coffee is a group of coffee shops that was established in 2008 in the United States. Founded in Staten Island, New York, Mrs. Susan and Mr. Mark Jones, business partners and friends for many years founded the company together and Mrs. Susan is the CEO and Mr. Jones is the President of Northside Coffee. A local spot for drinking coffee is Northside Coffee that serves freshly brewed coffee and espresso beverages, sweet baked goods, beer, and wine in the evenings and always enthusiastic baristas. Northside Coffee, like many small businesses, rely on a sound and hack-proof system to safeguard the business and customers. It is about the cybersecurity audit that considers the current state to understand strategies for protecting information and maintaining continuity of service in a coffee shop. Finding out critical risks and realistic enhancements, this audit is going to prepare the Northside Coffee against cyber threats. By means of specific recommendations, the audit helps the business to construct a stronger and more stable environment, oriented on its requirements and avoiding risks in a contemporary networked world.

Purpose

This cybersecurity audit aims to look at the security setting of Northside Coffee' computer and the networks plus its physical security and ways it manages its data. Through a critical analysis of each of these areas of concern, the audit seeks to determine the organizational risks which may lead to an undesirable compromise of organization's data integrity, confidentiality and availability. By doing so, Northside Coffee will identify sectors of possible risk and obtain guidance on strengthening cybersecurity for the whole company. The audit in effect aims at improving Northside Coffee protection against internal and external risks hence a safer operational territory.

Scope

This audit focuses on Northside Coffee' Internet connection, computers and critical data operations. Targets include open ports and firewalls, password regimes, malware precautions, and far more importantly, backup and recovery strategies. The physical security measures taken for controlling the accessibility to the computers, other hardware components and some other valuable resources are also discussed. Coordinated approach is devised to give an updated picture of the existing level of security both IT infrastructure and physical security of the coffee shop to counter threats from cyberspace.

1. What We Did

The audit team did the following to establish a structured assessment of Northside Coffee' cybersecurity measures:

Arrival and Initial Access: The team contacted the owner of the coffee shop that was being studied, Mark Jones, to get an access code. Further in, we noticed staff reactions to the unidentified entry as a physical intrusion prevention mechanism and staff attentiveness. There was no reaction from the staff to confirm our identities thus a call for better access measures.

Introduction and Audit Overview: Following from the entry assessment, our team greeted the owner and informed him about the audit and its characteristics. Altogether, we went through each of the audit items, strictly adhering to the work pattern set in out audit plan. More important, they interacted with the owner and other staff who needed to provide access to these systems and records.

Audit Activities: Each computer system, router, and relevant security protocol was checked against our audit criteria. The areas of focus included password strength, open network ports, system updates, malware protection, physical security safeguards, and device configurations.

Hot Wash and Findings Review: After completing the audit, we held a post-audit meeting with Jordan to discuss our initial findings. We agreed on some immediate next steps and discussed possible recommendations to address any significant vulnerabilities.

2. What are the Results

The audit revealed several areas of concern that, if addressed, would enhance the security and resilience of Northside Coffee' systems. Below are the key findings:

Weak Password Practices: Passwords were posted on visible sticky notes, and some passwords contained dictionary words, making them vulnerable to password-guessing attacks. These practices reduce password strength and increase the risk of unauthorized access. (See Item #1 on Audit Plan).

Open Network Ports: Port 80 was detected as open, exposing the network to potential external threats. Ideally, all ports should be in stealth mode to conceal network activities from unauthorized users. The current configuration may allow for unexpected access, representing a critical network vulnerability. (See Item #2).

Lack of a Formal Security Plan: Northside Coffee operates without a structured security policy, increasing the likelihood of inconsistent security practices and slower response to security incidents. Without standardized procedures, the organization is more vulnerable to both internal and external risks. (See Item #14).

Expired Malware Protection: The computer used for business operations lacked up-to-date malware protection, as the subscription to the existing software had expired. This gap in security leaves the system vulnerable to malware and viruses, which could compromise both data and system integrity. (See Item #8).

No Surge Protection: Equipment was plugged directly into wall outlets without surge protectors. In the event of a power surge, critical hardware could suffer irreversible damage, leading to potential data loss and operational downtime. (See Item #9).

Inadequate Physical Security Measures: The audit revealed that the main access door to the area housing computers was often left open, indicating poor physical security protocols. Physical security is a crucial aspect of cybersecurity; unauthorized individuals could easily gain access to sensitive equipment and data. The physical security of critical assets could be improved through the use of such features as keycard systems and biometric access to certain areas.

Unsecured Wi-Fi Network: According to the audit, the coffee shop has issued the improper network security of the Wi-Fi (for example, it does not have WPA3). An unsecured network means that there is a risk of listening to information that is passed over the network, the attackers may get to capture relevant information such as customer's information on payment. It is important for all wireless link to be encrypted with good encryption method to help safeguard customers' information.

Insufficient Employee Training on Cybersecurity: The results also reveal that organizational members do not undergo systematic training or sensitization on cybersecurity measures. Lacking proper training they can pose threats to the organization based on phishing attacks, social engineering or even improper handling of the data that the organization deals with. Applying the continual training can assist in increasing consciousness and revising proper use of computers by staff.

Risk Posture

Analyzing the results of cybersecurity risk assessment, the audit is to conclude that Northside Coffee operates in a *moderate risk area*, mostly because of a number of severe weaknesses detected during the process. Knowing these risks helps focus efforts to strengthen the organization's security profile.

1. Greatest Risks

- **Unauthorized Access**: The possibility of unknown persons gaining access to secure areas and equipment is very high. Just as in the Tributechop files, they use sticky notes for passwords, leaving the password exposed to anyone willing to type it, and open network ports provide space for cybercriminals to penetrate the organization. This risk is compounded by the absence of a formal security policy that would among other things set out the access control measures. *(The chance of hostile parties penetrating infrastructure or acquiring unauthorized access to networks is high. The findings revealed that many employees have habits of using easily guessable passwords, for example writing sticky notes on their desks and using open network ports provides several openings for the cybercriminals. This risk is increased by the absence of a professional security policy that normally outlines the access control standards).*
- **Data Breaches**: Since there is poor protection against malware and limited physical security measures, Northside Coffee is exposed to data theft risks. Hackers would be able to steal such customer data as their payment details or employee data as it is in the network with physical access to the tie and store it which would lead to loss of cash and reputation.
- **Operational Downtime**: Embodiment risks posed by operational outages, which can be caused by a cyber-event – ransomware attack or hardware damage due to power fluctuations and are pertinent. This further amplifies the exposure to effective disruptions to the business processes due to the absence of any precautionary measures on the computer system being used.

- **Legal and Regulatory Compliance**: Lack of proper measures to protect against cyber threats may cost Northside Coffee legal risks and may also suffer penalties in case customers' information is leaked out. Most countries have passed laws on data protection, which requires organizations to protect personal information; failure to do so exposes business to legal penalties.

2. Greatest Vulnerabilities

- **Weak Password Management**: The first weakness is as basic as using easily guessable passwords or writing passwords down where others can find them. This later on exposes the organization to password-guessing attacks and social engineering tactics making it easier for individuals to gain unauthorized access to the organizations critical systems.
- **Unpatched Software and Expired Security Solutions**: Malware protection on some of the system may not be updated while software may not be updated with latest patches making systems to be vulnerable to exploitation. There are new types of threats that appear from time to time, and if the system is not updated with new programs antivirus, Northside Coffee might suffer a malware attack that should have been avoided.
- **Inadequate Physical Security Controls**: It also provides no Keys and Locks, which are instrumental in preventing unauthorized personnel from accessing specific equipment and regions. Some of the impacts of physical breaches entail loss of IT hardware and data, which entails the need to enhance the physical security procedures.
- **Insufficient Network Security**: There is no network segmentation, implemented firewalls, or secure connection settings, thus making the network and its connected devices vulnerable to remote attack. This vulnerability can lead to interception of information and further compromise and exploitation of the system by other unscrupulous persons.
- **Limited Employee Awareness**: Insufficient staff knowledge of available security measures and general employee deficiencies in training directly impact an organization's vulnerability to human induced cyber threats. Failure to train employees periodically exposes them to phishing scams or increased risks of compromising critical information thus escalating organizational risk.

Therefore, the audit reveals the necessary risks and vulnerabilities that to insist to Northside Coffee to develop the cybersecurity strategy. Completion of the recommended actions will improve the organization security status and protect it from both internal and external threats and protect the organization datable.

3. What are the Recommendations

The following actions are recommended as measures towards addressing the vulnerabilities highlighted in the audit report: All the suggestions are made with a certain reference to an area of concern to avoid a significant awakening of organization's ongoing processes and in equal measure ensure that the costs incurred are minimum:

i. **Implement a Strong Password Policy:** Set a standard password policy that all employees must follow, including not being able to use any dictionary words for passwords. Staff should also refrain from writing down passwords in open areas that are easily observable by others. A possible solution is the implementation of a password manager, be it LastPass

or Bitwarden, in order to store passwords.
Timeline: Immediate (within 1 week)

ii. **Close Open Ports and Reconfigure Firewall:** Consult an IT expert to reconcile all the open but inactive ports and increase the firewall to make all the ports in stealth mode which very much minimizes the risks posed by external threats.
Timeline: Immediate (within 1 week)

iii. **Develop a Basic Security Plan:** Develop key activities which highlight measures that should be adopted on Passwords, security access and frequent update. Such policy will create unanimous view of the security and can be enacted utilizing the available templates with the minimal interference.
Timeline: Short-term (within 1 month)

iv. **Renew Malware Protection Software:** Replace or renew the old and expired software that has a malware protection capability. Hire cheap and durable products incorporating automatic update on security measures to ensure security is up to date.
Timeline: Immediate (within 1 week)

v. **Install Surge Protectors:** Buy power strips for some operational systems to protect the equipment from power surges. This little investment can save a great deal of equipment's and can also help avoid losses and ruin of important data.
Timeline: Immediate (within 1 week)

4. What is their Risk Posture

In terms of the cybersecurity risk applicable to Northside Coffee, the result indicated it was at a moderate level for several factors among them weak passwords, insecure network setting, and poorly defined security policies out rightly leaving the business at the mercy of hackers. The most severe weakness is the lack of a formal security strategy because the absence of a plan raises the risk of intentional and accidental security breaches. The above recommendations if put into operation will go a long way in strengthening the security of the organization, both physical and cybersecurity measures will be enhanced.

Conclusion

Northside Coffee cybersecurity audit identifies critical changes necessary to strengthen the organization's security stance. Major threats include weak passwords, open network ports, the lack of a formal security plan, malware protection that has expired, and no surge protection all weaken the confidentiality, integrity, and availability of the business's data and systems. Overcoming these threats with the help of recommended action plans will contribute to achieving the corresponding effect and minimize the probability of a breach. Using good passwords, setting appropriate network ports, creating a security strategy, reviving anti-virus software, and installing surge protectors serve best for less expenditure and can be carried out with little interruption. By doing so, this company will establish protective measures against internal and external threats and create a pathway to continued protection against cyber threats.

References

National Institute of Standards and Technology (NIST). (2020). *NIST Cybersecurity Framework*. https://www.nist.gov/cyberframework

Center for Internet Security (CIS). (2021). *CIS Controls v8*. https://www.cisecurity.org/controls/

SANS Institute. (2018). *Password Policy Recommendations: Best Practices for Organizations*. SANS Whitepapers. https://www.sans.org/white-papers/

Verizon. (2023). *Data Breach Investigations Report (DBIR)*. https://www.verizon.com/business/resources/reports/dbir/

Microsoft. (2022). *Guide to Improving Network Security*. https://docs.microsoft.com/en-us/security/