Risk Management

Juliette Richards

Unit 7, Assignment 1

IT2280

Professor Kuhlman

2/21/2025

Capella University

Table of Contents

Security Tools

To keep sensitive information safe within a company, various physical security measures are used. These include things like fingerprint scanners, security cameras, and special rooms for servers. Fingerprint scanners help confirm the identity of employees who need to enter restricted areas, reducing the chances of unauthorized access. Security cameras allow for ongoing monitoring and recording, which helps spot and look into any security issues that might arise. Furthermore, server rooms, where important computers and data are stored, can only be accessed by authorized staff. All these security tools work together to help protect important information and ensure it remains private (Naka Team, 2024).

Risk Assessment Strategies

Understanding and managing potential security risks is crucial for keeping a company's computer network safe. This involves regularly checking for weak spots that could be exploited by attackers. Companies use strategies like threat modeling and penetration testing to find these weaknesses. Once risks are identified, they are ranked based on how serious they are and what impact they could have. This helps organizations focus their resources on the most critical issues. It's also important for companies to continuously monitor and update their security measures to stay ahead of new cyber threats. By actively identifying and addressing these risks, organizations can strengthen their overall security and better protect sensitive information.

Security Policy

This security policy is designed to keep our company's information safe and secure. It provides easy-to-follow rules and steps to protect important data from unauthorized access, cyberattacks, and other risks. By sticking to these guidelines, we make sure we follow laws and regulations while creating a safe working environment for everyone.

Section 1. Security Policy Goals.

The purpose of this security policy is to protect the company's important information and systems. It aims to keep sensitive data safe from unauthorized access, data breaches, and cyber-attacks, while also making sure we follow necessary laws and regulations. Additionally, this policy is designed to ensure that the business can continue to operate smoothly by providing clear guidelines on how to secure data, control who has access to it, and respond to any incidents that may occur.

Sections 2. BYOD (Bring Your Own Device).

Employees can use their personal devices, like phones and tablets, for work, but there are important security rules to follow. First, they must register their devices with the IT department. Each device should also be protected by strong passwords and encryption, which is a way to keep information safe. If a device gets lost or stolen, it should have a feature that allows the company to erase all its data remotely to protect important information. Access to private or sensitive information is limited and regularly checked to ensure that data remains safe and confidential (NIST, 2020).

Section 3. AUP (Acceptable Use Policy).

This policy outlines how employees should use company internet resources. Staff members are not allowed to visit unapproved websites, download unauthorized software, or use the internet for illegal activities. The company’s network and resources should be used only for work-related purposes. If anyone notices anything unusual or suspicious, they should report it to the IT department right away. By following this policy, we help protect the organization from risks that come with misuse of our network resources.

Section 4. NDA (Non-Disclosure Agreement)

All employees and outside vendors must sign a Non-Disclosure Agreement (NDA). This agreement helps keep our confidential information safe and ensures that sensitive data isn't shared with people who shouldn't have access to it. By protecting this information, we safeguard our ideas and business details. If someone breaks the terms of the NDA, there could be serious consequences, including disciplinary actions and legal trouble (NIST, 2020).

Section 5. Password Policy

All employees need to follow the organization's password policy to maintain system security. Passwords must be at least 12 characters long, including a combination of uppercase, lowercase, numbers, and special characters. Multi-factor authentication (MFA) will be mandatory for accessing sensitive systems. Passwords must be changed every 90 days, and employees are not allowed to share passwords to prevent unauthorized access.

Section 6. Privileged User Agreement

Users with special access rights need to follow important security rules to keep information safe. This means they should keep a record of their activities and have regular check-ins to make sure everyone is following the rules and that no one is accessing data without permission. These users are responsible for what they do and must protect sensitive information to ensure it stays private and secure.

Section 7. Anti-Malware Policy

To keep our company’s computers safe from harmful software, all devices must have the latest antivirus programs installed. Regular checks and immediate protection are necessary to find and stop any potential threats. If you notice anything unusual or suspicious, please report it right away. Only apps that have been approved by the company can be installed on work devices to help reduce the chances of facing malware issues.

References

Naka Team. (2024, January 15). Protecting people and data: Crucial intersection of physical security and data privacy. Naka Tech. https://nakatech.com/physical-security-and-data-privacy/

National Institute of Standards and Technology (NIST). (2020). NIST special publication 800-53 revision 5: Security and privacy controls for information systems and organizations. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final