Introduction to Cyber Security Report

100384938 – John Callaghan
CMP-6039A/7018A

The Role and Implementation of Security Policies in Organizations

The National Cyber Security Centre defines Security policies as a set of rules that governs all aspects of security-relevant system and system component behaviour(NIST 2020). Meaning that they are essential to help defend against any security issues or threats being either internal or external. Along with that they act as a sort of rulebook for employees within the organization to follow. In the organization they are aimed towards both high level security objectives all the way down to day-to-day operations meaning they are applicable to all employees at any level within the company. The focus of these policies is to protect sensitive data along with ensuring employee safety and finally ensure that the company is being productive throughout the entire organization.

1 Importance of Security Policies

Security policies are important to companies for the following reasons:

- They provide guidance from higher-level employees to those with less access or permissions like developers or programmers ensuring that everyone fully understands security goals. For example, policies can determine who should have access to sensitive data and ensure access is controlled, such as through the Bell-LaPadula (BLP) model which takes all of those things into account.
- Policies give employees clear instructions on acceptable behavior, reducing errors and minimizing personal judgment. This results in increased productivity and efficiency, as employees always have reference points if they are confused.
- Having written policies helps organizations too comply with industry standards, such as ISO27001 (ISO 2022), a globally recognized certification for information security management. This certification ensures alignment with best practices and helps meet legal requirements like GDPR and NIS Regulations. It also reduces data breach costs by demonstrating to customers, partners, and stakeholders that steps have been taken to protect data, minimizing financial and reputational damage.

2 Protection of Organizations and Employees

2.1 Protecting Organizations

Throughout and clear security policies can help safeguard an organization's assets along with their employees in many ways:

1. **Identifying Critical assets:** Assets such as buildings, inventory, and sensitive data are prioritized based on their importance to the company.
2. **Protection measures:** Security protocols, including cybersecurity measures and linked protections, are implemented to address the unique needs of each asset.

3. **Disaster recovery plans:** Clear processes can help aid the business during emergencies like natural disasters, cyberattacks, or equipment failures which can help them get back to normal much faster.
4. **Helping to mitigate risks:** Regularly checking your business for vulnerabilities could assist in making decisions on protection and resource allocation.

2.2 Protecting Employees

Along with protecting a companies assets and the organisation itself security policys can also help employees by ensuring their safety and security:

- Regular training in cybersecurity and workplace safety protocols to prevent threats.
- Clear evacuation protocols for emergencies.
- Policies requiring best practices for password security and account management.
- Training employees to identify phishing emails, malware, and other threats, as employee training and the use of AI and machine learning insights were the top factors mitigating average data breach costs(IBM 2024). So its also applicable for your organisation aswell.
- Educating employees to recognize signs of suspicious behavior or compromised systems, such as checking audit logs.
- Ensuring employees know whom to contact if they suspect their accounts, devices, or data have been compromised.
- Clearly defining employee roles and responsibilities in maintaining security.

3 Ensuring Policies Are Being Followed

To ensure security policies are effectively followed:

1. **Appoint a Security Manager:** Hiring a Security Manager or Chief Information Security Officer (CISO) ensures continuous oversight of threats and compliance with security policies. They are responsible for things like monitoring risks and identifying suspicious activities or breaches. They also oversee the enforcement of policies across all departments, ensuring alignment with legal and industry standards. Additionally, the Security Manager plays a key role in coordinating incident responses and implementing corrective actions to prevent future issues.
2. **Regular Policy Updates:** Regularly updating security policies is essential to address evolving threats and changes in technology. Policies should be reviewed periodically, to ensure they remain relevant to current risks and regulatory requirements. Updates must also reflect new legal obligations, such as changes to GDPR or industry-specific standards, and adapt to emerging attack methods like AI-driven threats. Involving key stakeholders, such as IT teams and department heads, in the review process ensures comprehensive and practical updates.
3. **Employee Training:** Ongoing employee training ensures that staff understand and adhere to security policies effectively. New hires should receive on boarding sessions covering key topics such as recognizing phishing attempts, managing passwords, and reporting incidents along with regular refresher training helps employees stay informed about emerging threats and reinforces best practices.

Barts Marvelous Mart Insider Threat Security Policy

Purpose

This security policy outlines processes Barts Marvelous Mart can take to address insider threats and incidents that disrupt employees, customers, and assets. Insider threats may arise from intentional or unintentional actions by employees, contractors, or authorized personnel.

Information Risk Management

- All financial and customer data must be backed up daily and stored securely off-site. Store managers are responsible for ensuring daily sales data is properly uploaded and secured. Warehouse inventory systems maintain real-time backups of all stock movements.
- Before implementing any new systems or technology, a thorough security assessment must be conducted. This includes evaluating risks related to the current promotion freeze and staffing. The CISO must approve all new technology implementations.

Incident Management

- Each location must maintain an updated incident response plan that covers various types of insider threats. Managers and supervisors have to be trained on these procedures and know exactly who to contact in case of an incident.
- Recovery procedures must be documented and easily available to authorized employees. This includes data recovery and backups for system restoration. Each retail location and the warehouse facility must have a designated incident response coordinator.

Managing User Priviledges

- Access rights are strictly based on job roles and responsibilities. A cashier and any additional access must be approved by both immediate supervisor and IT security.
- When employees change roles or leave the organization, their access rights must be reviewed or revoked as soon as possible. Managers must immediately notify IT and Security when an employee departs. Along with temporary access privileges having to be automatically revoked after their time period ends.

Monitoring

- All system access should be monitored and logged, with more attention to sensitive areas like finance and inventory management. Unusual patterns such as accessing systems outside normal working hours or excessive transaction reversals, should trigger automatic alerts to security personnel.
- Security cameras monitor all retail locations and warehouse facilities 24/7. Camera footage is retained for 90 days and reviewed randomly by security staff. along with any gaps in coverage must be reported and addressed immediately.

Advice and guidance

- All employees regardless of role must complete the online security awareness training. The training is also role-specific for different areas of the company.

- Given the 24/7 warehouse operations and extended retail hours, security guidance must be accessible at all times. An online knowledge base is maintained with searchable security procedures and guidelines, accessible to all employees through their work credentials.

Secure Configuration

- All systems like corporate devices must run approved security software that updates automatically. Store managers and warehouse supervisors must verify daily that all systems are running current versions, with any outdated systems reported to IT immediately.
- Personal devices used for work purposes must have appropriate device management software installed. This is too ensure secure access to company resources while protecting sensitive data from potential insider threats.
- A comprehensive inventory of all hardware and software must be maintained across all locations and must perform regular audits of their technology assets and any missing or damaged equipment must be reported immediately.

Warehouse Security

- All warehouses must implement a strict visitor management system. All visitors must sign in and be accompanied by authorized employees at all times. Given the extended operating hours, designated staff members on each shift are responsible for visitor oversight.

Inventory Control Measures

- All stock movements between retail locations and the warehouse must be documented through the digital tracking system. Warehouse operators and stock managers must use individual login credentials when processing inventory, to ensure clear audit trails.
- Random inventory audits must be conducted weekly at retail locations and at the warehouse facility. Any issues must be reported to loss prevention and investigated immediately.
- Higher value items may require dual verification during receiving and shipping processes. This applies to both warehouse operations and retail store deliveries with warehouse staff cross-checking quantities and conditions.

Vehicle Security

- Delivery vehicles must be equipped with GPS tracking and digital locks that record all access attempts. Drivers must follow specific routes, with any deviations requiring immediate supervisor approval.
- Vehicle inspection protocols must be followed at the start and end of each shift. Drivers must document any damage or security concerns, and supervisors must verify these reports daily. All vehicles must be secured when not in active use.
- Loading and unloading procedures must be witnessed by supervisors and drivers must obtain confirmation for all deliveries and pickups, with electronic copies.

Disciplinary Procedures

- Security violations are categorized into three levels: minor infractions requiring retraining, serious violations resulting in formal warnings and supervision, and critical breaches leading to immediate suspension or termination. Each incident must be documented with evidence and witness statements where applicable.
- Discipline measures including mandatory additional training, increased supervision periods, and temporary restriction of system access privileges. All disciplinary actions must be reviewed by HR and the Legal department before implementation.

Data Protection Measures

- All sensitive customer and business data must be encrypted both in transit and when not in transit, with access restricted based on job roles and responsibilities. Regular data protection audits must be conducted to ensure compliance with privacy regulations and company policies.
- Employees are prohibited from downloading or storing company data on personal devices unless authorized to do so and using approved security software. Any data breaches or suspected unauthorized access must be reported immediately to the IT security team.
- Regular data backup and recovery tests must be performed to ensure business continuity in case of system failure or cyber attack. The CISO must review and approve all data protection procedures annually, with updates made to address new threats or vulnerabilities.

This policy will be reviewed annually to address evolving threats and operational changes. All employees must acknowledge their understanding and acceptance of this policy upon hiring and throughout their time at the Barts Marvelous Mart

4 Policy Review

The revised insider threat security policy for Barts Marvelous Mart covers multiple levels of insider threats by highlighting practical methods to secure the organization's operations. The policy uses things such as role-specific access controls, employee training, physical security measures, and ongoing monitoring making a very strong framework for mitigating all types of risks including insider threats. More specifically access restrictions for cashiers and warehouse workers ensure operations are able to run smoothly with a lower risk of these threats throughout daily operations, as well as system backups and mandatory reports. Continuous monitoring of system activity, 24/7 camera surveillance, and mandatory employee training can help in preparing for insider threat detection. Incident contingencies are further supported by simulations and designated coordinators, And processes such as recovery protocols minimize downtime. Dual-authentication access for sensitive areas and random inventory audits provide an added layer of physical and digital safeguards against insider threats making it harder for employees to make errors.

Limitations and Considerations

While the policy provides a lot of safeguards, due to current financial constraints on Barts Marvelous Mart it may be difficult for the company too implement all of these at once as these may require hiring more employees and upgrading technology, however it will be worth it as IBM reported in 2024 malicious insider attacks resulted in the highest costs, averaging USD 4.99 million dollars (IBM 2024). Which could prove beneficial as they would be safer in the long run by avoiding paying these large increasing sums of money if they paid to implement these features. Another thing to consider employees may be affected by morale due to the recent financial cuts on promotions. The employees morale may be lower which could also lead to an increase in insider threats as unhappy employees may feel unmotivated or resentment toward the company. This dissatisfaction could turn into intentional malicious actions or a poorer execution of security protocols. To mitigate this, the organization should also consider implementing other incentives and try to make better communication within the organization allowing the employees to feel more welcomed, which is not covered in the security policy, too ensure employees feel valued despite the financial constraints. Which could then lower the risk of these threats.

Conclusion

The policy shows an understanding of the organization's needs and details how to handle insider threat risks. It handles three of the most common insider threats being 1) data exfiltration, 2) violations against data integrity or availability and 3) sabotage of ICT systems(L Liu 2018) making it well suited for the majority of businesses as these are the main three issues they face. However, to deal with financial challenges, the organization could focus on trying to implement these cost-effective solutions like attempting to automate some security tasks following the trend of AI, As AI and automation is paying off, lowering breach costs in some instances by an average of USD 2.2 million(IBM 2024) Which shows how the new wave of AI can prove useful to save money for the company during these difficult financial times. Finally although there may be some methods that have not been covered within this policy it still covers most of the main threats and methods potential insiders could use to gain access to the company's systems and cause harm, Making it extremely useful for dealing with insider threats and ensuring the company is secure from these breaches.

5 References

1. Liu, L., De Vel, O., Han, Q.-L., Zhang, J., Xiang, Y. (2018). *Detecting and Preventing Cyber Insider Threats: A Survey.* IEEE Communications Surveys Tutorials, 20(2), 1397–1417. https://doi.org/10.1109/COMST.2018.2800740.

2. IBM. (2024). *Cost of a Data Breach 2024.* Retrieved from https://www.ibm.com/reports/data-breach.

3. McCallister, E., Grance, T., Scarfone, K. (2010). *NIST Special Publication 800-53 rev 5.* National Institute of Standards and Technology (NIST).

4. ISO/IEC. (2022). *ISO 27001.* IT Governance. Retrieved January 20, 2025, from https://www.itgovernance.co.uk/iso27001.

5. Addison-Wesley Professional. (2012). *The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* Retrieved January 20, 2025, from https://www.amazon.com/CERT-Guide-Insider-Threats-Information/dp/0321812578.