Policy Abstract

If there is any kind of suspicious or unauthorized access, or any type of security breach, Woolworths will follow appropriate procedures to identify, contain and recover from such events.

Office Responsible – Information Technology

Writer – Prakrit Roka

Introduction/Background

Security policy is an outline that shows the organizations' critical assets and loose ends and shows how they must be protected. It provides all the staffs the necessary information of the way of use of the organizations' assets. This helps the employees gain an insight in securing the organizations' information system.

Security policy is a must read for employees using the resources and system. When all employees know the guidelines they can follow necessary measures so the problem is solved efficiently and in as fast as possible. By discussing how information must be handled and how to respond to security breaks the organisation needs to address all the elements.

Security policies lay foundation of information security that explains employees how their actions account for protection of the sensitive information assets in the company. That is why they tend to create security policies. Protection of sensitive information is feasible when there are concrete controls and rules. Thus, standards, procedures and guidelines are implemented in the companies.

What are Standards, Procedures and Guidelines?

Specification on device configuration and installation, and softwares as well fall under standards. They describe how information and other aspects of organization are to be used. For example, the organisation may implement a password standard for its employees, as it will set out certain rules for password complexity and also Windows may implement a standard for hardening Window Clients.

Procedures give step by step instructions to perform various tasks that comply with policies and standards. They explain how to implement controls in affordable and easy manner. For example, an employee maybe given the task to install Windows operating system securely, so with the help of a written guide of procedures in how to install it, detailed steps will encourage the employee to ensure the operating system is secure to satisfy the policy, standards and guidelines.

Guidelines are advices that help achieve goals of security policy. They are only suggestions as it conveys best practices and conventions of a system. For example, a standard may implement that passwords should be 8 characters or more, so the guideline may state that there must be a best practice to ensure that the expires after 30 days. Another standard may set out control for accessing the internet securely but a guideline could be sent out to all employees in the form of a newsletter outlining the best practices for using the internet.

Date of Issue – 20th September, 2020

Maintenance

The policy will be yearly reviewed by the IT team and the head of department of Woolworths Group Limited. The policy might also be altered for improvement as recommendations of IT department.

Enforcement

In case of any kind of violations, there may be suspension or loss of violator's use privileges, with respect to organizations data. Additional administrative sanctions may apply up to and including termination. Civil, criminal and other similar remedies may apply.

Exceptions

Exceptions to this policy are to be approved by the Information Security Office and also formally documented. Policy exceptions will periodically reviewed for appropriateness.

Purpose

This paper provides general guidance and instructions that employees and managers of IT department can follow to:

- Quickly and efficiently recover from security incidents.
- Respond as a team and in a systematic manner to incidents.
- Secure sensitive data.
- Identify the cause of such incidents

Policies

1. Employee Credentials and Ids are not to be shared with anyone else.
2. Unregistered transactions are not to be carried out.
3. Client's information should be kept confidential.
4. In any of the business procces of the supermarket if there is suspicious act or breach the following procedures are carried out

    1. Identification:
       A dedicated team may identify a potential security breach through any internal or external complaint/notification, or other knowledge of unauthorized use of restricted data. Employee of the supermarket are to immediately report to help desk in case of suspicious activity or transaction. The reported issues should be made transparent to the Directors of the branch.

    2. Verification Phase:
       The detected issue needs to be verified by the IT department by checking with backups and also possibly going to the field where issue is reported from. There can be two possible senarios in this phase.
        1. The reported case may be false positive in which case the Director of the compromised system should write a brief summary of the incident for record and be available to all required employees.
        2. In case the case is true the level of threat is estimated and a team of security experts is deployed to investigate the compromised system.

    3. Containment Phase:
       This is the most contextually dependent and time sensitive phase of the investigation. The actions that need to be taken will depend on the level of threat the breach posses like uptime requirements of the compromised system, the suspected level of attacker privilege, the nature and quantity of data at risk, and the suspected profile of the attacker. The most important goals of this phase are to:

1. Eliminate hacker access: The first step is always to prevent furthur damage. In case of internal breach all the internal data flow needs to be halted and all clients need to be redirected to maintainence page. The impact of system downtime is not so high in supermarket but furthur data tamper may cause a huge toll. Incase of physical access, unsecure area must be secured.
2. Assess the detailed scope of incident by:
    - Listing compromised systems which can be different part of databases, server or physical devices.
    - Securing areas that may contain evidence.
    - Creating attack timeline based on available primary evidence.
    - Reporting police in case of physical breach.

4. Analysis Phase
   In this phase the in-depth investigation of the incident is done. The primary goal of analysis is to know weather the attack was successful and what kind of damage was aimed. The director of compromised should direct this phase. There should be proper examination on the damage the breach has done to the stakeholders. The following data must be analysed to make up a complete story of the breach.
    1. Suspicious Network Traffic: Is there any unidentified or unaccounted network traffic from suspicious region from where attack is carried out.
    2. Attackers Access to Data: Did the attacker obtain sensitive information that may harm the stakeholders.
    3. Method and Duration of Attack: How the incident occur and how long the attack went untraced.
    4. Attacker Profile: Is there any evidence that helps in identification of the attacker(s).

5. Recovery Phase
   Recovery phase should be done immediately after security has been optimized so that normal business is not greatly affected. Short term changes can be made to comprimised system to prevent instant risks.

6. Reporting Phase
   The final report must be made by director that serves two main purposes.
    1. The owners of supermarket should be briefly informed about the breach and damage done to the stakeholders and also how the incident was disclosed.
    2. A series of mid-term and long-term recommendations should be provided to improve security that prevents similar future breaches.

Potential Threats and Vulnerabilities of company's network.

There can be many ways by which the company's network can be breached. One of the major ways can be by carelessness of employees. Sensitive data like passwords of the internal network can be leaked through them. Similarly clients' sensitive information is also at risk due to employee's carelessness. Furthermore, the supermarket has some hardwares that are present within reach of people. The issues that can arise from this are hard to prevent but if the organization follows the above given policy, the breaches can be solved with least damage.

If above described policy is followed, the database cannot be altered by an external agent easily. The valuable information of clients will not be leaked too. There can still be scam

sites that can steal client information. These sites must be identified and disabled by the IT teams. There have been some incidents which have put the organization at risk.
On 2015 Woolworths supermarket unwillingly sent $1million worth of shopping vouchers to people who had purchased vouchers from deals site, Groupon. Woolworth was quick to rectify the situation. They must have followed protocol similar to the one described above. This is example of data leak due to employers' carelessness.
On 2018, Woolworths had tightened security around its loyalty program. This was because there were 130 cases in which Rewards accounts were accessed with valid login credentials that had been obtained from other sources or online scams possibly through social media. Woolworths said it had locked down hundreds of Reward online account with suspicious point redemptions. Woolworths then introduced five new controls and tools which prevented further cases of fraud giftcards.

Conclusion

No company is secure from cyberthreats. According to MediaPro report, one of the most vulnerable industry to cyberattacks are supermarket industries. IT teams are given the task of handling the security aspect but employees are the major loophole because they do not seriously read the standards and guidelines provided to them. Most organisations do not realise that their employees are violating the policy because firstly they have not read the document, believe they are doing nothing wrong, or the policy is just sitting in a cabinet to keep legal representatives happy. Security is not just IT issue but the issue of whole organization. A security policy doesnot, in itself, establish the requirements of a customer. It instead acts as a bridge between a flawless service between consumer and producer. A simple mistake can cause loss of millions for all stakeholders who are the suppliers, consumers, government, owners and many more. With small effort from the members the organization will mitigate many possible threats and also solve cases effectively.

References

SECURITY POLICY: WHAT IT IS, WHY AND CHALLENGES
Annureet Bajwa, Chaminda Hewage

Oct 04, 2019
<https://www.supermarketnews.com/retail-financial/hy-vee-says-malware-caused-payment-card-data-breach>

Keith Loria, May 16, 2017
<https://www.grocerydive.com/news/grocery--report-retail-is-the-most-vulnerable-industry-to-cyberattacks/535104/>

Sarah Homewood, June 2015
<http://www.adnews.com.au/news/woolies-data-breach-brand-damage-and-transparency>

Miranda Ward, Sep 12th, 2018
<https://finance.nine.com.au/business-news/woolworths-rewards-loyalty-scheme-scam-fraud-points/a2fdd210-8c74-4f82-a556-799a0bfa19d5>

<https://www.cmu.edu/policies/information-technology/information-security-policy.html>