



### Lab 2.1.2 Designing a Security Plan

#### Objective

In this lab, students will analyze, offer recommendations, and help improve the security infrastructure of a fictitious business. Students will complete the following tasks:

- Analyze business application requirements.
- Analyze security risks.
- Identify network assets.
- Analyze security requirements and tradeoffs.

#### Scenario

Widget Warehouse is a medium sized e-commerce company that supports 200 customers daily. The student has been hired to assist in the development of a new security policy. An assignment has been received to analyze the current network of Widget Warehouse. The Widget Warehouse network is comprised of an intranet with 200 users, and a public Web server that processes the company e-commerce traffic. The internal network is logically divided into an information technology (IT) department branch, an accounting branch, a customer service branch, a sales branch, and an inventory branch.

#### Preparation

To complete this lab, the students should have a firm understanding of the various security exploits that pose a risk to companies.

#### Tools and resources

The curriculum lists a number of excellent Web links that will help the student understand the material presented in these labs:

- Carnegie Mellon Software Engineering Institute or CERT <http://www.cert.org>
- National Institute of Standards and Technology Security Division or NIST <http://csrc.nist.gov/>

### Step 1 Create a list of various attack intruders

- a. The IT department for Widget Warehouse has a general understanding of security but they are very inexperienced with the various attacks an intruder can use to exploit their network resources. Create a list of various attacks intruders can use maliciously against the Widget Warehouse network. Also, provide a brief description of possible attacks, including their purpose.

Attack Name	Attack Description

## Step 2 Make a List of Security Requirements

- a. One of the first steps in creating a security policy is gathering the requirements for the company. Create a list of questions to ask the Widget Warehouse executives, in order to better understand their security requirements and business goals.

1. Widget Warehouse requirements.

---

---

---

---

---

## Step 3 Identify Security Implementation Options

- a. Based on the questions, it is discovered that mission-critical information is passed between remote departments in the company over the LAN and the Internet. What security implementation could be used to keep this information out of unauthorized hands? Provide a brief explanation with each answer.

---

---

---

---

---

---

---

## Step 4 Create a Description of the Security Wheel

- a. The Widget Warehouse executives do not completely understand the continual process of security. They appear to be under the impression that once a security policy is implemented it will be sufficient for an extended period of time. Create a description of the security wheel and discuss the benefits of such a model.

The security wheel is comprised of four steps:

Step Name	Step Description

### Step 5 Passive Monitoring

- a. The management of Widget Warehouse wishes to see some of the available options in security monitoring. As the consultant, suggest that a passive monitoring scheme may be an option they should pursue. Write a description of passive monitoring that is to be presented to Widget Warehouse management.

---

---

---

---

---

---

### Step 6 Explain Using a Security Policy

- a. Explain to the IT Department how using a security policy can provide advantages to the company as a way to secure sensitive information.
  1. Developing a security policy.

---

---

---

---

---

---

### Comments

---

---

---

---

---

---