Sri Lanka Institute of Information Technology
Introduction to Cyber Security
Lab Sheet 1
Year 2, Semester 1

Exercise 1: For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.

i. An organization managing public information on its Web server.
ii. A law enforcement organization managing extremely sensitive investigative information.
iii. A financial organization managing routine administrative information (not privacy-related information).

Exercise 2: Find out the applicable security controls to the following scenario.

Case Study: A Risk Audit of a Very Small Business

Introduction

The Business (as it will be referred to throughout this paper) is a very small business in its tenth year of operation. It has one full-time employee, the owner, and occasional part-time help from the owner's husband and various employees hired on a short-term "casual labor" basis. Last year the Business had under $100,000 in gross sales.

The Business is in the business of retail sales over a dedicated WWW site and via the mails. More specifically, it is in a niche market, one of only a handful of businesses in exactly this market on the entire Internet. Only over the Internet are their sufficient buyers for this business to be a full-time job. There are many companies like this in the United States.

Before

The first step in the audit was to get initial impressions and a general understanding of the Business, for context on what the owner told me. I toured the physical office setup and stock storage areas, and then followed some customer orders through the process from the customer through order fulfillment to records storage and retention.

Sri Lanka Institute of Information Technology
Introduction to Cyber Security
Lab Sheet 1
Year 2, Semester 1

The Physical Setup

The office for the Business is a single dedicated room in the owner's house, an outwardly unremarkable dwelling in a middle-class neighborhood.

The office has the following physical security: there is a deadbolt lock on the (solid core wooden) door. This lock is not on the same master key as other doors in the house. There are two 1' x 4' open-able windows, both of which are normally closed when the office is not in use. The house, which is 100' from its nearest neighbor and 50' from the road, has smoke alarms and external motion-sensor lights.

In the office are the following computers and equipment:

- A Macintosh G4 desktop computer ("the Big Mac") that stores the owner's and company's email, customer orders, and the Business's financial records.
- A gray-box PC used for personal use and for editing the website.
- An old desktop PC running Linux. This computer serves as a staging server for the website (the actual production site is offsite at a shared hosting facility).
- A Macintosh iBook laptop computer that stores the inventory database and the credit card authorization software (and hence a database of past credit card transactions).
- An HP LaserJet 4 network printer.
- A wireless/wired cable modem router/firewall appliance.

All but the iBook are connected together via normal category five network cabling; the iBook uses an Airport card to connect to the network and a modem to dial up the Business's credit-card authorization provider. All computers are using NAT and DHCP provided by the router and have IP addresses in a private IP range. There are no other computers connected to this network.

Stock is stored in filing cabinets and in plastic bins in the (attached) garage. The other half of the two-car garage is used for general household storage.

The Ordering Process: Web Orders

Web orders, which comprise over 90% of the Business's orders, come to the Business in the following way. A customer browses the Business's website, which is hosted on a shared server at a commercial hosting facility. This site is running an open-source shopping cart system written in Perl and heavily modified by the owner's husband. When the customer submits an order, the order is filed in an order log and two emails are sent. The customer gets an order summary (minus credit card information); the owner gets a terse note that says simply "You have an order, Boss."

The owner then FTP's to the server from the Big Mac and downloads the order log. After verifying that it looks correct and complete, she replaces the server's order log with a blank document. The orders in the order log are then split into separate documents, printed, and saved, named by customer name and order date, into an "Orders" directory on the hard drive of the Big Mac.

The printed copy of the order, containing all customer information, is placed onto an "Orders" clipboard.

The Ordering Process: Phone Orders

Phone orders, which comprise approximately 3% of the Business's orders, come to the Business in the following way. A customer calls the Business (on the Business's own phone line: the home phone is separate) and states that she wishes to place an order.

The owner or her husband grabs a scrap of paper (quarter sheets are kept near all Business phones) and writes down the order and all of the customer's information, including her credit card number. The order is then scotch-taped to the owner's computer monitor until it is placed onto the "Orders" clipboard.

The Ordering Process: Mail orders

Mail orders, which comprise approximately 3% of the Business's orders, come to the Business in the following way. A customer writes an order down and mails it to the Business with a money order. The Business hopes that customers use the written order form from the website for this purpose, but they do not more often than they do.

The owner places the money order in a bank bag for deposit and places the order onto the "Orders" clipboard.

Order Fulfillment

The owner (or an employee) takes the "Orders" clipboard to the garage, pulls from stock the required items, and brings them back to the office. If an item is not in stock, the order is placed on the "Back Orders" clipboard, and the customer is notified. For each order she fills, she creates a customer record (if there is none) on the iBook, opens the sale in the POS (point of sale) software, and runs the customer's credit card (if not mail order) in the credit card authorization module.

When the transaction is authorized, she closes the sale and prints two copies of the receipt. She then packages the order and uses the PC to create a mailing label. One copy of the receipt goes into the package; the other is retained for records. In the late afternoon of each day, the owner drives to the Post Office and mails all the packages. Order fulfillment is complete.

Data Storage/Retention

The owner takes the remaining copy of the receipt from each order, staples it to the order itself, and places them in a pile. At the end of the day, these orders and receipts are gathered, attached to the credit card settlement report, and filed by day in a file folder. Each month gets one or more labeled file folders, depending on volume; each year gets one or more labeled file boxes in the garage.

At the end of the day, the owner also goes through the receipts from the packages being shipped that day and moves the order files on the Big Mac into an "Orders Shipped" directory. These are kept forever, sorted by year, then by month, then by order date and customer last name.

The file boxes are kept on open wooden shelves in the garage for seven years, the record retention time specified by the Business's credit card service provider. At the end of that time, the files are shredded.

Policies

The Business has very few policies, all related to customers' orders and promises regarding customers' privacy. There were no other written policies or procedures. Employees, who are always casual laborers hired for the short term (when the Business gets a huge rush or the owner is otherwise getting behind), work under the owner's direct supervision, getting orders filled and out. They do not get or require keys or logins to the computers: when an employee is working, the owner logs herself into all computers that require it.