Qualitative Cybersecurity Risk Assessment of a Small Business

INTRODUCTION

Most security case studies focus on medium or large business organizations. The US Federal Government defines a small business as having fewer than 100 employees and, depending on industry, an annual income of less than a number ranging from $0.75 Million to $28.5 Million. Many businesses, however, are far smaller than that, but could still benefit from security awareness. This is a security audit of one such business. The Small Business (or SB as it will be referred to throughout this case) set up in a geologically stable area (College Station, TX), is a in its tenth year of operation. It has one full-time employee, Jessica the owner, and occasional part-time help from her husband Smith, and various employees hired on a short-term "casual labor" basis. Last year SB had $123,538.42 in gross sales. The business has been increasing at the rate of 10% (in terms of gross sales) for the last three years. This rate is expected to slow down to about 7% in the coming year. The IT budget of the business is generally around 5% of the gross revenues. SB is in the business of retail sales over a dedicated website and via the mails. More specifically, it is in a niche market, selling porcelain miniature collectibles. It is one of only a handful of businesses in exactly this market on the entire Internet. Only over the Internet are there sufficient buyers for this business to be a full-time job. SB is no different than thousands of other small businesses selling online in a niche market.

The Physical Setup

The office for SB is a single dedicated room in the Jessica'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' openable 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:

- An Apple iMac desktop computer ("the BigMac") that stores the Jessica's and SB's email, customer orders, and SB's financial records. The operating system on the machine is MacOS 10.12 Sierra.
- A Sony Vaio PC running on Windows 8. It is used for personal use, web browsing, and for editing the website.
- A Dell PC running Linux Ubuntu 18.10. This computer serves as a staging server for the website (the actual production site is offsite at a shared hosting facility).
- A MacBook Pro 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.

Additional technical details are listed in the following **TABLE.**

Computer Name/Description	Computer/Device Role
"**BigMac**": iMac running MacOS 10.12 Sierra	Owner's primary personal computer. Used for email and electronic order storage, as well as business financial records.
"**ThePC**": Sony Vaio. Running MS Windows 8	Used for personal use (e.g., web browsing) and for editing the website. No customer data. Runs the software "United States Postal Service's Shipping Assistant." This software allows the Business to print shipping labels for orders that already have the postal bar code on them, and to enable package tracking for Priority Mail packages at no additional cost.
"**Staging**": Dell desktop computer running Ubuntu 18.10	Used as staging server for the website. No customer data.
"**MacBook**": MacBook Pro laptop computer running Mac OS 9.2	• Used only by Jessica • Inventory database • Credit card authorization • All sales function when on road
Printer: HP LaserJet 4M with JetDirect card.	Printing • Paperwork • Shipping package labels
Router: D-Link router/firewall appliance	• Wired/Wireless Router 9802.11G) • Firewall • DHCP Server (to assign dynamic IP addresses to devices connecting to the network

All but the MacBook are connected via normal category five network cabling; the MacBook uses an Airport card to connect to the network and a modem to dial up the Business's credit-card authorization provider. All computers have dynamic 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 opens 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 BigMac 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 BigMac. 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 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 another 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

Jessica (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 MacBook, opens the sale in the POS (point of sale) software, and runs the customer's credit card (if not a 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 ThePC 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

Jessica 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, Jessica also goes through the receipts from the packages being shipped that day and moves the order files on the BigMac 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

SB 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 labor hired for the short term (when SB gets a huge rush or the owner is otherwise getting behind), work under the Jessica'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. Jessica's husband takes care of systems configuration and updates. He is always up to date with patches. The patches for Macs and Windows systems are done automatically, while those for the router are obtained from D-Link

Audit of the BigMac

General Items (not Macintosh-specific)
1. Is the computer backed up regularly? NO
2. Is the admin group restricted in membership? YES
3. Is an actual login required (disable auto-login) YES
4. Are there individual, named usernames for all employees? NO
5. Is display of all usernames restricted? YES
6. Is password strength appropriate? YES
7. Is a personal firewall configured? NO
8. Is an antivirus program installed and properly configured? YES
9. Is the physical case locked and secured? NO
10. Is theft-prevention software installed (MacPhoneHome in this case)? NO
11. Is the computer connected through a surge protector or UPS? YES
12. Is a locking screensaver configured? NO

Macintosh-specific items
1. Is the OS installed on a UFS volume, rather than HFS+? NO
2. Is an Open Firmware Password created and set? NO
3. Is access to NetInfo restricted? NO
4. Is the root account still disabled? YES
5. Is the system configured for at least weekly Software Updates? YES

Audit of ThePC (Sony Vaio)
General Items (not Windows-specific)
1. Is the computer backed up regularly? NO
2. Is the admin group restricted in membership? YES
3. Is an actual login required (disable auto-login) YES
4. Are there individual, named usernames for all employees? NO
5. Is display of all usernames restricted? YES
6. Is password strength appropriate? YES
7. Is a personal firewall configured? NO
8. Is an antivirus program installed and properly configured? YES
9. Is the physical case locked and secured? NO
10. Is theft-prevention software installed (PCPhoneHome in this case)? NO
11. Is the computer connected through a surge protector or UPS? YES
12. Is a locking screensaver configured? YES

Windows Items
1. Is the Guest account disabled? NO
2. Is the Administrator account renamed? NO
3. Is there a login warning message? NO
4. Are all drives NTFS? YES
5. Is the system currently patched to appropriate levels? YES
6. Is the system set for Automatic Updates and to ask the user if he/she wishes to install updates? YES
7. Is a BIOS password set? NO

Audit of the MacBook Pro

General Items (not Macintosh-specific)
1. Is the computer backed up regularly? NO
2. Is the admin group restricted in membership? YES
3. Is an actual login required (disable auto-login) NO
4. Are there individual, named usernames for all employees? NO
5. Is display of all usernames restricted? YES
6. Is password strength appropriate? YES
7. Is a personal firewall configured? NO
8. Is an antivirus program installed and properly configured? YES
9. Is the physical case locked? N/A
10. Is the laptop physically secured? NO
11. Is theft-prevention software installed (MacPhoneHome in this case)? NO
12. Is the computer connected through a surge protector or UPS? YES
13. Is a locking screensaver configured? NO

Macintosh-specific items
1. Is an Open Firmware Password created and set? NO
2. Is the system configured for at least weekly Software Updates? YES

Audit of the Router Appliance
The router appliance is a D-Link 624 AirPlus Extreme cable modem router. It has four standard twisted pair Ethernet ports and serves as an 802.11b/g wireless router, as well. It is also a firewall appliance and a DHCP/NAT server, as well. It is configured to run NAT, with all LAN clients getting private range IP addresses. On the WAN side, it obtains a dynamic IP address from the cable modem network provider.

1. Has the administrator password been changed? YES
2. Are ICMP ping requests blocked? NO
3. Is Remote Management disabled? YES
4. Is Remote Upgrade disabled? YES
5. Is IP address filtering enabled and functioning? NO
6. Is IP service filtering enabled and functioning? NO
7. Is MAC address filtering enabled and working? NO
8. Is Virtual Server disabled? YES
9. Are unwanted ports shut down to keep them from serving as a starting point of an attack? YES
10. Is logging configured and working? YES
11. Is the appliance plugged into a surge protector? YES
12. Is the firewall set to default Deny all connections from the Internet to the LAN? YES
13. Is the router set to obtain a dynamic IP address from the ISP, rather than a static one (if available)? YES
14. Has the wireless SSID been changed from “default”? NO
15. Has the wireless channel been changed from the default value? YES
16. Is the 128-bit WEP (Wired Equivalent Privacy) protocol enabled? NO

CYBERSECURITY RISK ASSESSMENT TASKS

1. Identify and define/describe **two** most critical business processes for this small business. Justify your choice of these business processes. **[6 Points] [NOTE:** *You will lose 3 Point if your justification is not convincing, e.g., not based on evidence/information in the case, is based on unrealistic assumptions, not clearly explained, copied from a friend's report etc*.]
2. Define a measurement scale(s) to score assets in terms of the impact of asset failure on the two business processes. **[6 Points] The measurement scale** should have the following three measures-
   CRITICAL: [*define critical in terms of operational impact of business process*]
   SUPPORTING: [*define critical in terms of operational impact of business process*]
   NO IMPACT: [*define critical in terms of operational impact of business process*]
   [NOTE: *You will lose 3 Point if the measures on your scales are not clearly defined in terms of impact of asset failure on the relevant business processes*]
3. Identify the IT assets that are critical or supporting in terms of the impact of their failure on the two business processes identified in STEP 1 **[10 Points]**. **[NOTE:** *You will lose 2 if you do not explain how an asset is critical or supporting to the one or both critical business processes*]
4. Identify at least 3 vulnerabilities and threats to the critical assets. **[10 Points] [NOTE:** *You will lose 2 Point per vulnerability-threat pair if the vulnerabilities are NOT based on information in the case, the threats are not valid or realistic for SB, unnecessary assumption are made, and/or you mislabel (e.g., exploit as vulnerability, impact as exploit, and/or impact as vulnerability etc.*].
5. Define the measures for the following threat likelihood scale and the threat impact scales. **[3 + 3 = 6 Points]**
   Threat Likelihood Scale: [*Highly Likely, Very Likely, Somewhat Likely, Not Likely*]
   Impact Scale: [*Very High, High, Moderate, Low*]
6. Provide the RISK MATRIX that you will use to score the risk the associated with each threat statement. **[2 Point] [NOTE:** *You will lose 1 Point the Likelihood and Impact measures on the threat matrix do not match the measures defined in STEP 5*].
7. Score the threat likelihood and threat impact scores for the threat statements obtained in STEP 4. **[2 Point]**
8. Provide the risk score for each threat statement identified in STEP 4. **[2 Point]**
9. What can the business owner do to mitigate her cybersecurity risks? **[6 Points] [NOTE:** *You will lose 2 Points if your suggestions are not specific to the computers and networking devices used by this business*]

Your Report will Lose Additional Points if-

1. There is evidence of plagiarism (as per Turnitin) **[-2 Points]**
2. All sources of information are not cited and referenced in the report **[-2 Point]**
3. There are spelling and grammatical mistakes **[-1 Point]**
4. Any assumptions made are not justified and/or clearly explained **[-1 Points]**
5. Miss the report submission deadline **[-5 Points**]

[**NOTE**- *If by some miracle a student ends up with a negative score then he/she will get a zero for the assignment*]