Global Information Assurance Certification Paper

Case Study: A Risk Audit of a Very Small Business

Doug Browne
GSEC Practical,
Version 1.4b, Option 2
Submitted September 11, 2003

Case Study: A Risk Audit of a Very Small Business

Table of Contents

Abstract

Many security case studies focus on large businesses, or on small businesses, for limited values of "small." 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.[1] Many businesses, however, are far smaller than that, but could still benefit from security awareness.

This is a security audit of one such business, focusing on the discovery and risk analysis process. This paper describes the environment, determines and assesses risks, and addresses the risks that we found. At the start of this process, the biggest known risk was uncertainty, the "We don't know what we don't know" factor. Therefore, this paper will focus on the discovery and risk analysis process, and provide technical details in appendices.

[1] SBA, Question 2.

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 there sufficient buyers for this business to be a full-time job. There are many companies like this in the United States.[2]

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.

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' 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:

- 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.

Additional technical details are listed in Appendix 1.

[2] This is not the point of this case study, but in 2000 (the last year for which data was available), there were 1.7 Million nonemployer businesses (without regular employees) in the retail trade in the United States, and they accounted for some $73 Billion of revenue (SBA, Nonemployer Statistics).

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 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

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 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 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 labor 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.

During

I started by sitting down with the owner and laying out the following high-level procedure, adapted from those of the National Institute of Standards and Technology and SANS[3]:

1. Determine what must be protected (assets)
2. Identify and define possible threats to those assets
3. Determine and prioritize the risks.
4. Assess responses to the risks.

She agreed with this procedure, and we started with determining assets.

Determine what must be protected (assets)

According to the Business owner and her husband, the significant assets of the Business are as follows (in alphabetical, rather than priority, order):

- The Computer systems
- Customer information (on those computer systems and elsewhere)
- Customer relationships and the Business's reputation
- The knowledge and skills of the owner herself
- Miscellaneous fixtures and equipment.
- Paper records
- The stock (items for sale)
- The website

Only some of these assets would be valuable to a competitor or a cracker, usually the first thought when threats, risks, and vulnerabilities are discussed, but each is at risk to one degree or another in terms of one or more of the classic "CIA Risk Triad" of Confidentiality, Integrity, and Availability.[4]

Identify and define possible threats to those assets

Possible threats are manifold. In order to prioritize the threats, we need to determine the likely impact of each threat, as well as its likelihood. "Impact measures the level of 'pain' to the organization," and "Likelihood measures the probability of feeling the impact."[5] We also need to have an idea how good our information is on these subjects – uncertainty is an unavoidable part of analyzing and dealing with risks. In this case, since everyone who works for the Business can be gathered in one room for discussions (and they were), we can be confident in the information available from the staff. The likelihood ratings for outside action and acts of God are still, unfortunately, best estimates.

There are two basic approaches to finding threats: vulnerability-driven and asset-driven.[6] The vulnerability-driven approach requires defining all possible vulnerabilities,

[3] NIST and SANS, respectively.
[4] Benson.
[5] Kimmelman, slides 25, 26.
[6] Kimmelman, slide 27.

a difficult task to say the least, while the asset-driven approach allows the assessor to go through the assets, one by one, defining what could threaten the Confidentiality, Integrity, and/or Availability of that asset. For that reason, this approach has been chosen for this study.

In this approach, we list, for each asset, the various threats to its Confidentiality, Integrity, and/or Availability. Then we assign each threat a High, Medium, or Low Impact rating and a High, Medium, or Low Likelihood. This is a process that requires experience, and is, by definition, at least partially subjective: what is a "high medium" rating to one assessor may be a "low high" to another.

In order to improve clarity, the threats identified are listed in Appendix 6, the Threat Table.

The computer systems:

The computer systems are a locus for risks, as so much information resides on them. Like the computers at many small businesses, they are not backed up according to best practices. They effectively form the largest single point of potential failure for the Business.

A cracker "0wn1ng" the Big Mac could download the orders from thousands of customers, including their credit card information, and do who knows what with it. This is a threat with a very high impact. Determining the probability required a separate audit – See Appendix Two. The Big Mac's OS is relatively secure, but not completely. Macintosh root exploits are also a lot rarer these days than PC ones,[7] and the Big Mac is behind the firewall.

A cracker "0wn1ng" the PC would have far less information. No customer information is stored on the PC, so there is little to take. He could, however, use the PC as a Distributed Denial of Service (DDOS) "zombie host" of some sort, which would be detrimental to the Business's network and reputation. Determining the probability required a separate audit – See Appendix Three.

A Macintosh virus could theoretically take out both the Big Mac and the iBook, forcing them to be rebuilt from scratch and causing the loss of all data on them. This would have a major impact on order production, but not as bad as it might; the current orders are all printed out on the "Orders" clipboard. The loss of financial records would be a bigger problem. However, the likelihood is comparatively low: there are comparatively few Macintosh viruses in the wild these days. In addition, the owner keeps Norton Antivirus up to date religiously on both Macs; she does not, as a matter of policy, open email attachments from strangers; and the Business's computers reside behind a simple, tough firewall.

A PC virus is much more likely, as there are a lot more of them out there these days. However, it would have much less impact on the Business. The only Business data stored on the PC is a complete copy of the website, which is duplicated on the staging server and which can be replaced quickly and easily onto any computer with an FTP client. Only in the event that it happened simultaneously with the hosted website going down and the staging server having an issue would this be a crisis. In addition,

[7] Harley (section 6.0) states that there about 40 Macintosh-specific viruses and root exploits as of the time he wrote, and not all of them were active; the Wildlist (Wildlist) indicates confirmed reports of 234 PC viruses actively infecting PC's in the world in July of 2003 (the most recent statistics available).

the owner's husband (the PC's primary user) keeps Norton Antivirus up to date and keeps up to date with Microsoft operating system updates as well.

A hardware problem with the Big Mac (such as a bad hard drive) would have a high impact on the Business, because, once again, data is not backed up. The hardware could be quickly replaced (there is an Apple Store in town), but the data on the hard drive would not be so easily replaced. The Big Mac is currently four years old; the hard drive was upgraded in 2001, and Apple makes good hardware. This makes the likelihood low, but it increases every year.

A PC hardware problem (such as a bad hard drive) has about the same likelihood, as the two machines have identical Maxtor IDE 100 GB replacement hard drive. However, due to the lack of vital information on that PC, it has a lower impact.

A hardware problem on the staging "server" (such as a bad hard drive) would have nearly zero impact in the short run. The owner and staff would simply route website updates around it and avoid making large changes to the site until the server was replaced.

A fire in the office that destroyed the computers and records could be a disaster. This could cause total loss of the computers, the data on them, and the order information on the "Orders" clipboard. Even if the stock was all right, the owner could be in the position of having no idea what to send, and to whom to send it. Business records on the Big Mac would probably be gone, as well. This could be a business-ending catastrophe. Thankfully, this is unlikely. The house is well built and well maintained, and there are smoke alarms and three fire extinguishers in the house.

An electrical surge due to lightning, utility issues or other reasons is, unfortunately, more likely. This could destroy or make useless computers and all records on them. The order information on the "Orders" clipboard would be OK, and orders can be mailed without official laser-printed US Postal Service labels, so orders could go out, but business financial records would be gone. In order to help prevent this, all the computers in the office are connected to uninterruptible power supplies (UPS's), which should protect them from such a surge. This makes the likelihood of the computers being damaged in such an event low (non-zero, but low).

Computers being stolen in a break-in could be a catastrophe. Not only would customer data be lost (availability), but it would also, potentially, be made public (confidentiality). This would create a risk of identity theft for thousands of customers. This is not highly likely, however, as the house is in a good neighborhood and has motion sensor-controlled exterior lights, the office is locked when not in use, and the computers are all several years old (making them appear less worth stealing).

The iBook being lost or stolen while the owner is traveling would have a huge impact. There are all those customer credit card numbers on the hard drive (confidentiality), and it is not backed up anywhere (availability). The loss of the iBook hardware is comparatively minor. This is a very real risk, as the owner does travel, publicizing the business and meeting with vendors.

A cracker intercepting customer data as it travels over the wireless network could have a high impact to customer data confidentiality. However, the likelihood is low: the house is 100' from its nearest neighbor and 50' from the road: there is no place to hide while waiting for this elusive customer data to come across the network. The lack of

Wireless Encryption Protocol (WEP), however, should be addressed as a matter of best practices.

A cracker intercepting customer data as it travels over the cordless phones could, in theory, have a high impact to customer data confidentiality. However, the likelihood is low: the house is 100' from its nearest neighbor and 50' from the road: there is no place to hide while waiting for this elusive customer data to come across. A "can you hear me now?" field test indicated that the phones could not reach to the road. In addition, the business averages one phone order per week, each lasting five to 10 minutes: listening here would simply not be worth the time and effort. Cellular telephones are not, as a rule, used for business at the Business Office.

Customer information
(On the computer systems and elsewhere):

Customer information being stolen from the web server before the owner gets it is a potential nightmare. This threat to the confidentiality, integrity, and availability of customer information has a huge potential impact: a typical order has a credit card number, name, and billing address. This is limited somewhat by the owner's efforts to download orders promptly, limiting the number of orders on the server at any one time. The likelihood of this threat being realized is probably medium. The server is well secured and the owner's husband has heavily customized the site's open source code for security. However, new exploits come out weekly and there are still frequent attempts to get the order log based on a shopping cart exploit that the owner's husband patched over two years ago.

Order information being stolen from the Big Mac or the iBook by an employee and ultimately used for identity theft is another nightmare, for all the same reasons. The likelihood of this, however, is low. The owner knows employees for a while before she hires them, and they generally work closely with the owner and in the same room.

Loss of customer information availability due to computer problems at the Business office is a large, multi-faceted problem that is addressed under computer systems.

The Business's customer relationships and reputation:

Like those of all retail businesses, customer relationships and reputation are very important to the Business. The Business needs to appear knowledgeable, get orders out promptly, and satisfy customers' needs. There are several possible threats to different aspects of this asset.

Confidentiality of the Business's customer relationships is not a large factor, as the Business does not sell things that would generally hurt a customer's reputation, but that is a potential threat. A list of the Business's customers being given to a competitor (by a disgruntled employee, for example) would make the Business appear to have poor security covering customer data, making customers reluctant to do business with them. It is not very likely, however. Not only do employees generally work closely with the owner and in the same room, but it would be easier for competitors to obtain lists of potential customers legitimately from various interest organizations than it would be to steal the Business's.

Orders going out late would threaten both the integrity and the availability of customer relationships: if customers were angry about this, they would tend to tell their friends, and much of the Business's business comes from word-of-mouth. The likelihood of this, however, is low, as the Business is pretty organized and the customers are generally reasonable. The website is also clear about establishing reasonable expectations.

A competitor or former customer slandering The Business could have a very low impact on the integrity of the Business's reputation, or a high one, depending on the distribution of the false information. The likelihood of this, however, is low: the Business's competitors are few, and most customers are happy with the Business.

An advertised item becoming no longer available would have a medium impact on the availability of the Business's customer relationships and the integrity of its reputation, as it would appear to be advertising what it could not deliver. However, most customers understand that this can happen, and the Business never charges a credit card until after the order is pulled from stock and ready to ship, so the impact is limited. This has to be rated a medium probability, as well, as it has happened in the past, and some of the Business's vendors are not the most reliable vendors in the world about ship dates.

A phone order being lost and never found, or found too late, could be a big problem. This is a problem with the integrity of that customer relationship, and the availability of the information. In many cases, it may also make that particular customer unavailable, as well, as they take their business elsewhere. This is a medium to high likelihood: quarter sheets of paper are easy to lose and it has certainly happened before.

The knowledge and skills of the owner herself:

The owner's personal skills and knowledge are very important to the Business's success. One of the factors in the Business's reputation is her knowledge of the stock and of how to make it work for customers' specific needs. Her husband and the part-time employees have absorbed some knowledge through osmosis, but cannot help customers the way that she can.

For this asset, confidentiality is not a factor: she gives the knowledge away to anyone who asks. The integrity of the asset is not a large factor: she usually has enough knowledge to reject false new information. If she were to pass on bad information, however, this could significantly hurt the Business's reputation.

The availability of this asset, however, is more of a factor. The owner's health is not exactly perfect, and she spent some time in the hospital the previous year. During that time, her husband got the orders out, but he could not answer customer's technical questions. This had a cascading effect on another asset: customer relationships.

Miscellaneous fixtures and equipment:

The miscellaneous fixtures and equipment stored in the garage[8] are theoretically vulnerable to fire and flood (availability and integrity), but the likelihood is low. This is

[8] Examples include fabric racks hand-made from 2x4's, sheet metal greeting card display racks from the 1930's, and the like. While these are assets to the Business and would have to be replaced if destroyed or stolen, they are useless to 90+ percent of the general population.

not likely, as the garage and house are well built and well maintained. There is also a (physical) firewall between the house and garage, and smoke detectors and fire extinguishers readily available. A flood is significantly less likely than a fire to have real impact on the Business, as there is a forty-foot deep ravine ten feet behind the house, ensuring excellent drainage, to say the least.

A break-in, likewise, would be unlikely to affect them, as, in the event of a successful break-in, they would probably not be seen as being worth stealing.

Paper records:

The paper records stored in the garage would potentially have a huge impact if stolen, as this could expose thousands of customers (seven years worth) to potential identity theft. Losing the records would also create a vulnerability to credit card chargebacks and IRS audits. However, this is unlikely: the house does not look out of the ordinary and the Business records look like the boring business records that they are.

Losing the paper records to a fire or flood would have much less impact: the only impact this would have is creating a vulnerability to credit card chargebacks and IRS audits. Ironically, the destruction of the records would make the Business's customers safer, as the records could not then be stolen. As with losing stock to these potential disasters, however, both fire and flood are unlikely.

The stock:

A fire in the garage could destroy all the Business's stock (the items for sale) at once, making it impossible for the Business to continue until new stock could be obtained, and costing the Business thousands of dollars in stock replacement costs. This is not likely, however, for reasons already described.

A flood, likewise, could destroy much of the Business's stock at once. A good bit of the stock is stored in plastic totes that would protect the stock and would even float. They are also stored on shelves above floor level. However, a flood is significantly less likely than a fire to have real impact on the Business, as there is a 40' deep ravine ten feet behind the house, ensuring excellent drainage, to say the least.

A break-in to the garage could theoretically be a problem, as stock could be stolen. However, the house does not look out of the ordinary and the Business sells in a niche market: the stock cannot be readily pawned or fenced. The trailer used to haul stock to trade shows was broken into last spring, and the thieves took nothing: they looked at the stock and saw nothing that they perceived to be of value. Therefore, this actually causing the business significant pain is a low likelihood.

The website:

The website itself is a significant asset, as the majority of the Business's orders come through the website and the majority of the rest are facilitated by it (these people typically "just don't want to put their credit card information online"). The website's integrity or availability becoming compromised would be a potential crisis.

A cracker defacing the website, which, interestingly, has not yet happened, would be a medium impact. Customers would be unable to place orders, and they certainly would not get a favorable impression of the Business's technical acumen, but the site is

selling products, not the Business's technical acumen. Most customers would come back. This, however, is not a likely event. The website is well known only in a small niche retail market, and is hosted at a hosting provider who is responsive about security patches and procedures.

The website becoming unavailable due to a Denial of Service attack or other "forces of nature" on the Internet is a risk with some impact, and it is quite possible. This is, after all, the Internet.

The hosting provider going out of business or being inaccessible to the Internet in the long term would have a greater impact, as it would probably take longer to resolve. It would take a day or two to re-route DNS, at the minimum, even if the owner instantly chose another hosting provider and transmitted the code. Order loss is also possible. This, however, is not greatly likely.

Miscellaneous Threats:

There a few threats to all physical assets that do not fall neatly under just one category above. An earthquake, for example, could destroy the entire house and its contents in one fell swoop (very high impact to availability of all physical assets). However, the Business is set up in a geologically stable area (central Ohio), so this is unlikely. A tornado could do the same, but the Business is in an area that sees few tornados,[9] making this unlikely as well. Since the Business is over 1000 miles inland, hurricanes are likewise only a theoretical threat.

Determine and prioritize the risks

"Risk is the chance that a threat will have an impact on your company."[10] One common way of thinking of it is "Impact X Likelihood = Risk."[11] In other words, risk is how much you need to worry about a particular threat, as it is the combination of the amount of pain the threat will cause if it happens and how likely the threat is to happen.[12]

We will use a qualitative model for this threat analysis, rather than a quantitative one, as it is easier to perform. This model is readily applicable to a broader spectrum of business risk than only information.[13] A best-practices model is applicable to some of the areas of the Business under review, but there do not seem to be best practices defined for all of the business process areas that we must examine.

Now we simply go down the list, generally averaging the impact and likelihood ratings for each threat. Nothing, however, may be rated higher for risk than its impact

[9] This county saw 21 tornados in the span 1950-1995, and they did a total of $6.6M in property damage. This should be compared with 65 tornados and over $260M in the same period in Lubbock County, Texas, part of "Tornado Alley." (NOAA).
[10] NIST, p. 17.
[11] Kimmelman, slide 23. This type of pseudo-mathematical statement is more usually used in quantitative analyses, but the concept is valuable no matter what type of analysis you are doing.
[12] Definitions from Kimmelman, slides 25 and 26.
[13] Bass and Robichaux, pp. 64-66. This is not to say that others are not broadly applicable, as well.

rating: if something is not going to hurt much when something happens, it is not a huge risk. Anything that has a high impact is at least a medium risk, if not a high risk.

The Risk ratings for all of the listed threats are found in Appendix 6: Threat Table. No attempt has been made to create an absolute priority list of the threats here: the information is insufficiently precise for that.

Assess responses to the risks

> A balance must be found between too much security (very restrictive use, high cost) and too little security (unrestricted use, low visible cost, but high danger). It is important that the value of the information and processes in the system is determined, and the risks identified, so that appropriate countermeasures can be implemented.[14]

An organization can make three basic responses to a risk, once they have identified and defined it.[15]

The first is to accept the risk and work on other things. This is often the best approach for very low risks or ones about which the organization cannot effectively do anything. The risk of a drummer spontaneously combusting is an example: this has a very low likelihood, so bands tend to accept this particular risk and work on things they can more easily affect, like perfecting their lyrics.

The second is to try to mitigate the risk. This means trying to reduce the risk by reducing the potential impact, reducing the likelihood that it will affect the organization, or both.[16] For example, you patch your server, thus reducing the likelihood that the new exploit for your OS will affect you.

The third is to try to transfer the risk. This means that you get someone else to accept at least some of the risk for you. For example, you buy business insurance.

There are no other responses to a risk: anything else boils down to one of these three or a combination of two or more of the three. Bass and Robichaux, for example, identify seven risk control mechanisms:

1. Avoidance: all risk is by-passed by deciding not to process, store or maintain the information [or other asset]
2. Transfer of assets outside the risk area: Assets at risk are moved outside the risk boundary.
3. Reduction of threat: Mechanism(s) put in place to reduce threat.
4. Reduction of vulnerability: Mechanism(s) put in place to reduce vulnerability.
5. Reduction of criticality or mission impact: Alter process(es) to minimize risk.
6. Detection: Analysis of logs, audit trails, intrusion detection systems, etc.

[14] FEMA, p. 19
[15] SANS, slide 6-3.
[16] Remember: Impact X Likelihood = Risk.

7. Recovery: Appropriate level of backup and recovery processes and mechanisms.[17]

Avoidance (not processing, storing or maintaining the asset) is simply transferring the risk to whoever has the asset (or to no one if the asset is destroyed, discarded, or abandoned). Transfer of assets outside the risk area is one way to mitigate the risk: move the asset to where the risk does not affect it. Reduction of threat, vulnerability, and criticality/mission impact are all different ways to mitigate risk. Detection is not, in my opinion, a response to risk all by itself: rather, it is part of a strategy to respond to a potential threat.[18] Recovery, likewise, is part of a strategy to reduce the impact of a threat (thus mitigating the risk).

Bass and Robichaux's model is, however, still useful, as it identifies the basic methods to mitigate risk. Where this study recommends mitigating risk, the specific Bass & Robichaux method will also be specified.

Appendix Six lists the identified threats, identified by asset and by the risk level (High, Medium, or Low) assigned in the previous step.

What I found when I went through all the risks was that a few recommendations effectively addressed many of the risks. These recommendations were mostly best practices that big companies do as a matter of course, but that home-based businesses often neglect. The Business had already implemented many of these, but not all. The recommendations that I made to the Business owner are listed in Appendix 7.

Business insurance allows the Business to transfer the risk of stock losses (for whatever reason), damaged, destroyed, or stolen computer equipment, fires, floods, tornados, hurricanes, and other acts of God. The liability component helps protect the Business from the legal liability impact of customer data losses. A data recovery clause even protects the Business somewhat from hard drive death. The Business already had adequate insurance in place.

Backing up all the Business's important data is vital, and was simply not happening at the Business. Like many small businesses, the Business had grown gradually, and no one had ever gotten around to implementing a backup plan. This became item #1 on the recommendation list. It mitigates risk from hardware problems, viruses, crackers, stolen computers, human error, and countless other potential risks.

No old data had ever been archived, another characteristic mistake of small and home businesses. Having a computer record ready to hand of every order the company has ever filled is rarely, if ever, necessary. In addition, when the company is almost ten years old and has thousands of past orders, it exacerbates most confidentiality risks, simply because there are so many more customers whose data can potentially be lost. Archiving that data to CD-ROM or other media and removing it from the computers will not only reduce the impact of confidentiality and availability risks by a huge margin, but it also reduce the impact of integrity risks (the owner can go look up old data if she needs it, and know that it has not changed).

[17] Bass and Robichaux, p. 66.

[18] It is possible to adopt detection as one's only response to a risk; this amounts to acceptance of the risk, since one is not attempting to prevent the pain.

Physical security measures were actually fairly good at the Business, for a home-based business. The dedicated office with a lock on the door is a simple thing that affects this more than the owner had thought about. For example, babysitters and workers can be in the house without necessarily having access to the office. The Business also had smoke detectors, fire extinguishers, UPS's, motion sensor-activated exterior lights, and the like. Assets were stored pretty well as far as flood potentials were concerned (stock in plastic totes on shelves).

However, both stock and paper records were in the garage, with no additional protection from a fire or break-in. I recommended that the Business owner find a way to protect both stock and paper records from both fire and break-in, but this recommendation was met with the problem of cost. Fireproof lockboxes large enough to protect the 10.5 cubic feet of business records[19] are certainly available.[20] However, enough fireproof safe space to protect the 200+ cubic feet of stock is just not economical for a business this size.

The alternative chosen was a locking cabinet for the business records. The measures already in place for the stock (plastic totes, being up on shelves, and business insurance) will have to be sufficient. The Business owner chose (correctly, in my opinion) to accept the (fairly low) risk of having her stock stolen or lost in a fire, rather than pay for a mitigation method that would cost her more than she could afford.

In addition, I recommended physical defense in depth for the computers: physically securing the computers so that they would take more than a moment to pick up and remove from the premises. The owner accomplished this with industry-standard PC cables, manufactured for the purpose.

Computer security was a large task, and these audits and the specific recommendations made for each computer and the router are documented in Appendices 2 through five.

Because of the danger of lost orders, I recommended the creation of a half-page form, printed on colored paper, for phone orders, and the placement of copies beside all store phones. Once a phone order is taken, the order can be placed directly on the "Orders" clipboard, and this should reduce the risk of loss. The colored paper, too, should help prevent the forms from getting lost in the shuffle. This is decidedly "low-tech" information technology, but it suits the Business's budget and addresses the problem. A copy of the form has been reproduced at the end of Appendix 7.

After

The Physical Setup

The office, at first glance, has not changed much. The same computers are on the same desks in the same room. However, the owner has changed the configuration of all of them to one degree or another, and they are now all physically secured to the desks. All the computers have locking screen savers, and they all now require individual logins in order to use them.[21]

[19] Seven boxes, times 1.5 cubic feet each.
[20] Some fireproof gun cabinets come to mind, for example.
[21] See Appendices 2-4 for details.

The largest physical change is the addition of an external USB CD-burner on the Owner's desk next to the Big Mac. Using this, the owner backs up customer data from both the Big Mac and the iBook and archives it to CD-ROM.

Stock is still stored in plastic bins on shelves in the garage. Paper records, in the same boxes as before, are stored in a locked wooden cabinet in the garage.

The Ordering Process: Web Orders

The ordering process for web orders has not changed significantly.

The Ordering Process: Phone Orders

Phone orders still come to the Business in the same way. The owner or her husband writes down all of the customer's information, including her credit card number and CVV (Credit Verification Value, that last three digits on the back of your credit card that merchants have started asking for), on a Phone/Mail Order Form, and place the order onto the "Orders" clipboard.

The Ordering Process: Mail orders

Mail orders still come to the Business in the same way. The owner or an employee copies the order onto a Phone/Mail Order Form, making sure that all the necessary information is there. She then places the money order in a bank bag for deposit and places the order onto the "Orders" clipboard.

Order Fulfillment

Order fulfillment has not changed significantly.

Data Storage/Retention

Data Storage and Retention, on the other hand, has changed significantly. 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 a locked cabinet in the garage.

At the end of the day, the owner goes through the receipts from the packages being shipped that day and moves the appropriate order files on the Big Mac into an "Orders Shipped" directory. She then copies the credit card files from the iBook over the network into a subdirectory named by date in the same directory on the Big Mac. With a click of one icon, she then backs the (encrypted) directory to her iDrive, a service provided by Apple for backups.[22]

Only two past months worth of these files are archived on the Big Mac and the iDrive. At the end of each month, the owner verifies that the month's credit card files from the iBook are all on the Big Mac. She then deletes the credit card files from the iBook.

[22] This creates a risk, because there is now customer data, albeit in an encrypted form, outside the Business's direct sphere of control. The owner felt that the reduced risk of data loss was worth the comparatively low risk of data cracking on the iDrive. The iDrive is in her name, not in the name of the business. Her husband has access to it, in the event that she were unavailable.

She burns all three month's worth of these files (from both computers) to each of 2 CD-ROMs, tests the burn, labels the CD-ROMs with the date range included, and takes one CD-ROM to her in-laws' home.[23] She then places the other CD-ROM in an old fireproof safe in the closet of the office and deletes the least recent month's files from the Big Mac and the iDrive.

The file boxes with the paper records are kept in a locked cabinet 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

There are not many policies and written procedures at the Business, even now, but there are a few. Anyone using a computer will log in with her own account or with an account named for her job ("OfficeAssistant", for example). Employees, who are always casual labor hired for the short term (when the Business gets a huge rush or the owner is otherwise getting behind), are hired from a small pool of college students and other chronically under-employed people whom the owner knows personally and trusts. They still work under the owner's direct supervision, getting orders filled and out. They do not get or require keys.

Conclusions

The lessons learned from this audit of one particular very small business can be applied to many, if not most very small businesses. Very small businesses tend to be in more danger from environmental factors and "stupid human tricks" than from crackers, as they do not have the resources simply to absorb the damage from a fire or from a particularly bad human error. This is not to say that they are not vulnerable to crackers as well, but the various risks must be viewed in the context of all of the risks to the business.

Very small businesses typically have some very characteristic security issues, and they always have very small budgets available for security changes. That does not mean, however, that very small businesses cannot or should not apply the same principles of risk analysis and security used by large corporations, scaled to their needs and the resources available.

[23] Her in-laws live in another suburb of the same city. They simply have a shelf of these CD-ROMs on a bookcase in their home office. The CD-ROMs do not have the business name on them, only the date range. The owner decided that the security advantages of having an offsite backup copy outweighed the additional confidentiality risk caused by this backup copy.

References List

At Stake. LC4. URL: http://www.atstake.com/research/lc/download.html (September 10, 2003).

Bass, T. and Robichaux, R. "Defense-In-Depth Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations." October 28-31, 2001. URL: http://www.silkroad.com/papers/pdf/defense-in-depth-revisited.pdf (September 5, 2003).

Benson, Christopher. "Security Strategies." 2000. URL: http://www.microsoft.com/technet/security/bestprac/bpent/sec1/secstrat.asp (September 6, 2003).

Charnick, Earl. "Getting the Most Security out of the Linksys Cable/DSL Router." February 12, 2003. URL: http://www.sans.org/rr/paper.php?id=619. (September 10, 2003).

Deal, Daniel. "Mac OS X 10.1.4: Security Analysis and Recommendations" June 4, 2002. URL: http://www.sans.org/rr/papers/34/241.pdf (September 8, 2003).

Federal Emergency Management Agency (FEMA). "Toolkit For Managing The Emergency Consequences Of Terrorist Incidents, Appendix D: Cyberterrorism" February 11, 2003. URL: http://www.fema.gov/pdf/onp/toolkit_app_d.pdf (September 6, 2003).

Gibson Research Corporation. "Shields Up! Port Authority Edition – Internet Vulnerability Profiling" October 21, 1999. URL: https://grc.com/x/ne.dll?bh0bkyd2. (September 10, 2003).

Harley, David. "Viruses and the Mac FAQ." August 23 2003 URL: http://www.faqs.org/faqs/computer-virus/macintosh-faq/ (September 7, 2003).

Juran, Joshua. "PortXTender." August 31, 2003. URL: http://www.metamage.com/products/port-xtender/. (September 8, 2003).

Karagiannis, Konstantinos. "Ten Steps to a Secure Wireless Network." February 25, 2003. URL: http://www.pcmag.com/print_article/0,3048,a=36109,00.asp. (September 9, 2003).

Kimmelman, Jeff. "Risk Assessment and Management." April 17, 2002. URL: http://www.issa-ne.org/documents/IT_Risk_Assessment_Methodology%20.pdf (September 6, 2003).

Libbenga, Jan. "CD-Rs deliver degrading experience." January 9, 2003. URL: http://www.theregister.co.uk/content/54/32593.html. (September 7, 2003).

Microsoft Corporation. "Microsoft Knowledge Base." 2003. URL: http://support.microsoft.com/default.aspx?scid=fh;EN-US;KBHOWTO. (September 10, 2003).

Microsoft Corporation. "Microsoft Windows XP Security Guide." 2003. URL: http://go.microsoft.com/fwlink/?LinkId=14840. (September 10, 2003).

National Institute of Standards and Technology (NIST). "Information Security: Defining Your Needs." URL: http://sbc.nist.gov/PPT/3-Defining_Needs_Notes.PDF (September 5, 2003).

National Oceanic and Atmospheric Administration (NOAA) "Storm Events." August 11, 1998. URL: http://www4.ncdc.noaa.gov/cgi-win/wwcgi.dll?wwevent~storms (September 7, 2003).

Roberts, Aron. "Personal firewall software for the Mac OS." September 4, 2003. URL: http://seaotter.berkeley.edu/cab/mac-firewalls/. (September 10, 2003).

SANS Institute. "Security Essentials III: Internet Security Technologies: Risk Management and Auditing, v. 1.8" August 2002. (September 8, 2003).

Schrader, Dennis. "Microsoft Windows XP Home Edition Security Implementation." December 13, 2002. URL: http://www.sans.org/rr/papers/67/974.pdf (September 10, 2003).

SecureMac.com, "Security Auditing Tools for the Macintosh." 2002. URL: http://www.securemac.com/secauditing.php. (September 8, 2003).

Security Consensus Operational Readiness Evaluation (SCORE). "Terms of Use Agreement." 2001. URL: https://www.cisecurity.org/sub_form.html. (September 10, 2003).

Shavlik Technologies. HfNetCheckPro, v.4. URL: http://www.shavlik.com. (September 10, 2003).

Small Business Administration (SBA). "Frequently Asked Questions." May 13, 2002. URL: http://app1.sba.gov/faqs/faqindex.cfm?areaID=15 (September 7, 2003).

Small Business Administration (SBA). "Nonemployer Statistics." March 25, 2003. URL: http://www.sba.gov/advo/stats/data_nepdf.xls (September 7, 2003).

Watkins, Steve. "Setting up a Firewall in OS X." February 26, 2002. URL: http://lowendmac.com/practical/02/0226pf.html. (September 8, 2003)

Wildlist Organization (Wildlist). "PC Viruses In-the-Wild-July, 2003." July 2003. URL: http://www.wildlist.org/WildList/200307.htm. (September 7, 2003)

Appendix One: Computer Details

Computer Name/ Description	Computer/Device Role	Recommendations Made/ Resolution of Recommendations
"Big Mac": Macintosh G4 desktop computer. Running Mac OS X (10.2.1).	Owner's primary personal computer. Used for email and electronic order storage, as well as Business financial records.	See Appendix Two
"ThePC": Gray-box PC. Running Microsoft Windows XP Professional.	Used for personal use and for editing the website. No customer data.	See Appendix Three
"Staging": Old Compaq desktop computer running Mandrake Linux 8.5	Used as a staging server for the website. No customer data.	Backups, if this can be accomplished quickly and easily. Otherwise none.
"iBook": Macintosh iBook laptop computer running Mac OS 9.2	• Inventory database • Credit card authorization • All sales functions when on the road	See Appendix Four.
Printer: Hewlett-Packard LaserJet 4M with JetDirect card.	• Printing, both paperwork and package labels	Just keep it running.
Router: D-Link router/firewall appliance	• Wired/Wireless Router (802.11G) • Firewall • DHCP Server	See Appendix Five.

Appendix Two: Audit of the Big Mac

Auditing a Macintosh is more difficult for most administrators than auditing a PC, due to a comparative scarcity of both automated tools[24] and best practices documents, checklists, and other such tools. I started this checklist with Daniel Deal's excellent analysis in his "Mac OS X 10.1.4: Security Analysis and Recommendations."[25] I wrote this checklist so that all answers should be "Yes."

Item	Yes	No
General Items (not Macintosh-specific)[26]		
Is the computer backed up regularly?		X
Is the admin group restricted in membership?	X	
Is an actual login required (disable auto-login)	X	
Are there individual, named usernames for all employees?		X
Is display of all usernames restricted?[27]	X	
Is password strength appropriate?	X	
Is a personal firewall configured?[28]		X
Is an antivirus program installed and properly configured?	X	
Is the physical case locked and secured?[29]		X
Is theft-prevention software installed (MacPhoneHome in this case)?		X
Is the computer connected through a surge protector or UPS?	X	
Is a locking screensaver configured?		X
Macintosh-specific items		
Is the OS installed on a UFS volume, rather than HFS+?[30]		X
Is an Open Firmware Password created and set?[31]		X

[24] To be fair, I downloaded a security audit tool called MacPork 2.0 from the SecureMac site (SecureMac, "Auditing"), but I could not get it to run on either the Big Mac or the iBook. I was unable to locate any other Macintosh-specific automated scanning tools (I am sure, though, that many of the UNIX tools will work, to one degree or another).

[25] Deal. I have added items which Deal did not mention

[26] These are best practices, no matter what OS you are running.

[27] One option in the Mac OS interface is to have the user, instead of typing in her username, simply select from all the usernames configured on that Mac. From a security point of view, this is, obviously, a very bad thing.

[28] Like many other versions of BSD, OS X ships with a personal firewall capability. This can be configured using the ipfw ruleset language, or a variety of applications will configure it for you. One of the most commonly recommended is Brian Hill's Brickhouse (Deal, 20, and Watkins). Watkins gives step-by-step instructions for installing and using Brickhouse.

[29] This is physical defense-in-depth.

[30] Deal strongly recommends this. However, as he says on the same page,

> …the only genuine problem will persist only as long as Classic applications continue to be used: the type/creator code scheme used to associate documents with applications in Classic will not function if Mac OS X is installed on a UFS volume. If a user of Mac OS X relies on Classic applications, the convenience of launching these applications with a simple double-click on a document in Finder may outweigh the benefit of improved security that the UFS filesystem offers. (p.3).

The owner uses several classic applications (for which she has found no OS X-native replacements) in the operation of her business. This makes this not a good option for her, so I did not recommend it.

[31] Deal, p. 7.

Item (continued)	Yes	No
Is access to NetInfo restricted?[32]		X
Is the root account still disabled?[33]	X	
Is the system configured for at least weekly Software Updates?	X	

I recommended that the owner address each item flagged above:

- Create a plan to back up all significant data on this computer on a regular basis. This goes hand in hand with the recommendation, already made, to archive old customer data that is no longer necessary.
- Create individual named accounts for each employee, or at least an "OfficeAssistant" account and an account for the owner's husband. Require through policy that users of this Macintosh use the correct named account. This will allow for tracking and accountability. It will also allow the owner to place Business financial data, for example, off limits to temporary employees by means of file system and application permissions. When the accounts are created, restrict access to NetInfo.
- Install Brickhouse and use it to configure the Big Mac's personal firewall. This will allow for defense in depth in the office.
- Physically secure the Big Mac in the office to help prevent a burglar from easily walking off with it. This includes locking the case, to prevent component theft/damage.
- Configure a locking screensaver to prevent someone from using the Mac without logging in.
- Install MacPhoneHome. This software sends the owner an email every time the Mac boots up, with the Mac's serial number and its current IP address. It also works in the firmware to prevent reinstallation of the operating system, or booting from a CD-ROM. This includes setting an Open Firmware Password.

[32] Deal, p. 14.
[33] Root ships disabled in MacOS X, but administrators can enable it. This is rarely a good idea (Deal, p. 19).

Appendix Three: Audit of the PC

I was much more comfortable auditing the PC, due to having much more personal experience with PC's, as well as the comparative abundance of security resources for Windows.

The PC is used in the Business only to run a single piece of software: the 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. The loss of Availability of this machine would be bad, but it would not be a crisis.

Item	Yes	No
General Items (not Windows-specific)[34]		
Is the computer backed up regularly?		X
Is the admin group restricted in membership?	X	
Is an actual login required (disable auto-login)	X	
Are there individual, named usernames for all employees?		X
Is display of all usernames restricted?[35]	X	
Is password strength appropriate?[36]	X	
Is a personal firewall configured?[37]		X
Is an antivirus program installed and properly configured?	X	
Is the physical case locked and secured?[38]		X
Is theft-prevention software installed (PCPhoneHome in this case)?		X
Is the computer connected through a surge protector or UPS?	X	
Is a locking screensaver configured?	X	
Windows Items[39]		
Is the Guest account disabled?		X
Is the Administrator account renamed?		X
Is there a login warning message?		X
Are all drives NTFS?	X	
Is the system currently patched to appropriate levels?[40]	X	

[34] These are best practices, no matter what OS you are running

[35] One option in the OS interface is to have the user, instead of typing in her username, simply select from all the usernames configured on that PC on the "Welcome Screen." From a security point of view, this is, obviously, a very bad thing.

[36] I verified this with LC4 (formerly known as L0phtcrack). See below.

[37] Windows XP ships with a personal firewall included, the Internet Connection Firewall (ICF).

[38] This is physical defense-in-depth.

[39] This list was started from Dennis Schrader's "Microsoft Windows XP Home Edition Security Implementation," and then I added additional items from my own experience.

[40] I verified this with Shavlik Technologies' HfNetCheck Pro (see below). This tool should be used, rather than exclusive reliance upon Windows Update, as, in my experience, HfNetCheck is less likely to miss a patch.

Item (continued)	Yes	No
Is the system set for Automatic Updates and to ask the user if he/she wishes to install updates?[41]	X	
Is a BIOS password set?		X

I used a number of free utilities that made this job much easier:

- Shavlik Technologies makes a free "Special Edition" of their industry standard product HfNetCheckPro, though registration is required. It can be downloaded from Shavlik at http://www.shavlik.com/pProducts.aspx. This version will scan up to 10 workstations and 1 server for patches, and allow you to click a button to install them. This tool is wonderful, and this limited capacity is plenty for a truly small business.
- At Stake makes a limited version of LC4 (formerly known as L0phtcrack) available at http://www.atstake.com/research/lc/download.html. This 15-day free download will do user information, dictionary, and hybrid attacks; brute force attacks require licensing the software. Registration was not required.
- While I was not permitted by the Terms of Use to use them for this audit,[42] SCORE, a joint effort between SANS and CIS, has some excellent checklists and tools available at https://www.cisecurity.org/sub_form.html. I would recommend them.

I made the following recommendations, and the owner agreed:

- Back up this computer. Even though there is no customer data on this PC, it would be inconvenient for it to be out of commission due to a problem.
- Create individual named accounts for each employee, or at least an "OfficeAssistant" account, an account for the owner, and an account for the owner's husband. Require through policy that users of this PC use the correct named account. This will allow for tracking and accountability. It will also allow the owner's husband to place his personal information off limits to temporary employees by means of file system and application permissions.
- Install and configure IPF, the free firewall software that comes with Windows XP. This took less than five minutes, and, since the PC is not

[41] The procedure for doing this may be found at http://www.microsoft.com/windowsxp/pro/using/tips/maintain/autoupdates.asp. Schrader expresses no opinion on which of the three options (ask before download, download then ask, or automatically download and install) for Automatic Updates is preferable. I am expressing one: automatically installing whatever patch a vendor says is important without checking it out first is dangerous and creates a completely new set of risks that are beyond the customer's control.

[42] "Receipt of the CIS download package components does not permit you to: … Post the Benchmarks, software tools, or associated documentation on any internal or external web site…[or] Represent or claim a particular level of compliance with the CIS Benchmarks unless [conditions which I could not meet in this audit]." (SCORE, 2: Limitations on Use)."

supposed to be a server of any sort, it locked down many common IP and UDP ports to prevent them from being used in any kind of attack.[43]

- Install and configure ZoneAlarm, a free personal firewall software package that is highly recommended by many analysts. Between the virus protection, firewall appliance, and the personal firewalls, the PC can be said to be defended in depth.
- Lock and secure the physical machine, to keep a burglar from walking off with it. This includes locking the case, to prevent component theft/damage. This is physical defense in depth.
- Install and configure PCPhoneHome. This software sends the owner an email every time the PC boots up, with the PC's serial number and its current IP address. It also works in the firmware to prevent reinstallation of the operating system, or booting from a CD-ROM. This includes setting a BIOS Password.
- Disable the Guest account, to prevent its use. This account, which by default has no password, is rarely useful. I also recommended giving it a strong password, in case the account were to be enabled somehow later.
- Rename the Administrator account. This account should never run without being renamed, as it is too tempting a target.
- Create an appropriate login message. This is rarely going to be a legal issue, since anyone who has legitimate physical access to the PC may use it for the Business (and, presumably, anyone who does not have legitimate physical access should know that they're not supposed to use the PC), but the effort expended to do so is small.[44]
- Set a BIOS password. This protects basic settings from change, either accidental or malicious.

[43] The exact procedure is in the Microsoft Knowledge Base at http://support.microsoft.com/default.aspx?scid=kb;EN-US;283673.
[44] The exact procedure is in the Microsoft Knowledge Base at http://support.microsoft.com/default.aspx?scid=kb;en-us;315232.

Appendix Four: Audit of the iBook

I originally thought that my recommendation on the iBook would be a two-minute "slam dunk": "You're using Mac OS 9! Get an OS with some significant security!" This laptop computer does not require a login for use, has an unencrypted hard drive, and, because of MacAuthorize, the credit card authorization software, it holds literally thousands of credit card numbers.

However, it was not nearly so simple. Because of the kernalized way in which OS X is written, non-native OS X applications cannot directly access most of the hardware. To be more specific,

> Applications which, instead of running natively in Mac OS X, run in the Classic compatibility environment do not have access to the internal modem. One such example is MacAuthorize, an application for processing credit card transactions. MacAuthorize requires an available modem for contacting the financial networks, and while it otherwise works fine in Classic, the inability to use the internal modem poses a problem.[45]

MacAuthorize must, in order to work properly, dial the credit card service provider directly for every credit card transaction (or for every batch, when operating in store-and-forward mode).

This started a give-and-take discussion, the kind that security audits so often involve.

So upgrade… MacAuthorize, which the Business has been using for years, is one of very few credit card authorization software packages currently available for the Macintosh. The assets of Tellan, the company that wrote MacAuthorize and its counterpart, PCAuthorize, were sold to ICVerify, which was sold to Verisign, who do not support MacAuthorize. There will be no new versions that support Mac OS X.

So switch applications… All Mac OS 9 (non-native OS X) applications will have the same problem. There is one application (AuthPayX, from Parallel Software) currently commercially available for Macintosh OS X that has the features that the Business needs.[46] Licensing would cost approximately $1000.00 for the one workstation, a large sum for a very small business.

*So go to Windows, a nice Windows XP laptop***…** The users, ultimately, must accept all security solutions, in order to the solutions to be successful. The security people will get the owner's Macintosh from her when they pry it out of her cold, dead fingers. Since she has been using Macintoshes for so long, the interface and way of thinking is very ingrained. The owner refused to accept a Windows-only solution or a Linux/UNIX-based one, other than Mac OS X. In addition, she quite rightly pointed out the costs of this solution: a new laptop plus Windows versions of her point of sale software, financial software, and credit card authorization software packages. This solution would cost several thousand dollars, which is more than AuthPayX would cost.

---

[45] Juran.

[46] There any number of Web-based credit card authorization systems. However, the Business cannot use these at trade shows, where they must sometimes store-and-forward credit card transactions for as long as three days at a time. This means that these systems do not meet the Business's needs.

So use an adapter… It would be possible to use an external modem through a serial-to-USB adapter to connect to one of the Mac's USB ports. However, this solution is physically fragile and awkward. On the road, it would create more risks, in terms of the unavailability of credit card services, than it would prevent.

But there must be a way… There may be. "Port XTender is a software serial port bridge between Mac OS X's Classic environment and the internal modem that is standard equipment on all shipping Macs."[47] This software, which costs only $100, will, if it does what it promises, allow the use of MacAuthorize with Mac OS X. The owner has downloaded a trial copy and is going to test it on the Big Mac before making a purchase decision.

But that's practically shareware… This is the financial environment of the very small business. If a $100 piece of software will do the trick, perhaps with some modification of a business process, it is far superior for the Business's purposes to a $1000 piece of software that does exactly what the Business needs. This is where the very small business differs from the 80-employee, $20M/yr "small business."

Once it was determined that moving to OS X was not an immediate option, I proceeded to audit other things on the iBook, and I had some recommendations for the owner. This checklist is the same one used for the Big Mac, with the OS X-specific items removed (the different hard drive formats, for example, are not an option in OS 9).

Item	Yes	No
General Items (not Macintosh-specific)[48]		
Is the computer backed up regularly?		X
Is the admin group restricted in membership?	X	
Is an actual login required (disable auto-login)		X
Are there individual, named usernames for all employees?		X
Is display of all usernames restricted?[49]	X	
Is password strength appropriate?	X	
Is a personal firewall configured?[50]		X
Is an antivirus program installed and properly configured?	X	
Is the physical case locked?	N/A	N/A
Is the laptop physically secured?[51]		X
Is theft-prevention software installed (MacPhoneHome in this case)?		X
Is the computer connected through a surge protector or UPS?	X	
Is a locking screensaver configured?		X
Macintosh-specific items		
Is an Open Firmware Password created and set?[52]		X
Is the system configured for at least weekly Software Updates?[53]	X	

[47] Juran.
[48] These items are best practices, no matter what OS you are running.
[49] One option in the OS interface is to have the user, instead of typing in her username, simply select from all the usernames configured on that Mac. From a security point of view, this is, obviously, a very bad idea.
[50] MacOS 9 does not come with a personal firewall, but they exist as commercial software.
[51] This is physical defense-in-depth.
[52] Deal, p. 7.

I recommended that each item flagged above be taken care of, and the owner agreed to the following steps:

- Create a plan to back up all significant data on this computer on a regular basis. This goes hand in hand with the recommendation, already made, to archive old customer data that is no longer needed.
- Configure the iBook for Multiple Users (the Macintosh mechanism for requiring a login). Ensure, when she does it, that users are required to type in a username rather than select a user icon.
- Purchase and install a personal firewall. There are several available for Mac OX 9.[54] This will allow for defense in depth in the office. Without it, there is not even defense in shallowness when the Business is on the road.
- Physically secure the laptop in the office to help prevent a burglar from easily walking off with it. Physically secure it when selling on the road, as well, for much the same reason.
- Configure a locking screensaver to prevent someone from using the Mac without logging in. This is particularly important on the road, where the physical security of the house is absent.
- Install MacPhoneHome. This software sends the owner an email every time the Mac boots up, with the Mac's serial number and its current IP address. It also works in the firmware to prevent reinstallation of the operating system, or booting from a CD-ROM. This includes setting an Open Firmware Password.
- When and if the iBook is converted to OS X, it will need a new audit before it goes "into production."

[53] Deal, p. 21.
[54] Roberts, "Personal firewall products for Mac OS 8 & 9."

Appendix Five: 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.

Though it is not a perfect fit, I used the outline for "Getting the Most Security out of the Linksys Cable/DSL Router"[55] created by Earl Charnick as my starting point. The reason I used this document is that the D-Link and the Linksys routers are analogous in form and function. I simply had to add auditing the wireless components that the Linksys lacks.

Item	Yes	No
Has the administrator password been changed?	X	
Are ICMP ping requests blocked?		X
Is Remote Management disabled?	X	
Is Remote Upgrade disabled?	X	
Is IP address filtering enabled and functioning?		X
Is IP service filtering enabled and functioning?		X
Is MAC address filtering enabled and working?		X
Is Virtual Server disabled?[56]	X	
Are unwanted ports shut down to keep them from serving as a starting point of an attack?	X	
Is logging configured and working?[57]	X	
Is the appliance plugged into a surge protector?	X	
Is the firewall set to default Deny all connections from the Internet to the LAN?[58]	X	
Is the router set to obtain a dynamic IP address from the ISP, rather than a static one (if available)?[59]	X	
Has the wireless SSID been changed from "default"?[60]		X
Has the wireless channel been changed from the default value?	X	
Is the 128-bit WEP (Wired Equivalent Privacy) protocol enabled?[61]		X

[55] Charnick.
[56] Virtual Server is D-Link's term for allowing a server on the LAN to function as a server on the WAN, serving HTTP, FTP, SMTP, Telnet, or the like, through IP pass-through. This creates a vulnerability, so it is best to have this disabled unless it is necessary. In this case, the owner has no use for this service, so it should be completely disabled.
[57] This item and the items above it are all from Charnick, pp. 6-7.
[58] This means that virtually all non-requested connection attempts to the LAN will be blocked by the firewall.
[59] This means that the LAN is a moving target for crackers: each time the router obtains a new DHCP lease, there is a chance that it will have a new external IP address. This will not work, obviously, if you are hosting a website or other Internet service, but, since the Business is not, it works just fine, and is cheaper to arrange with the ISP.
[60] Karagiannis.
[61] Karagiannis.

Based on this checklist, I made the following recommendations:

- Set the router to block incoming ICMP ping requests, as these are often the starting point for an attack.[62] The owner agreed to this.
- Review setting up filtering on the router to prevent users (or other processes with access to the computers on the LAN) from accessing known bad sites. The owner did not feel that this was necessary, but would reconsider if a problem developed.
- Change the wireless SID from "default." The owner agreed to this, as long as I could make it work with the iBook.
- Change the wireless channel from its default value. The owner agreed to this, as long as I could make it work with the iBook.
- Enable 128-bit WEP. "Passively cracking the WEP (Wired Equivalent Privacy security protocol is merely a nuisance to a skilled hacker …Still, the protocol does at least add a layer of difficulty."[63] The owner agreed to this, as long as I could make it work with the iBook.

A tool that I found very useful in testing the firewall was Gibson Research Corporation's "Shields Up!" Internet vulnerability profiling software.[64] It can be found at Gibson's site: https://grc.com. This allowed me to remotely check which IP ports were vulnerable from the Internet (virtually none), which made it easier to verify that the firewall was doing what it said it was.

[62] Charnick, pp. 4-5.
[63] Karagiannis.
[64] Gibson.

Appendix Six: The Threat Table

Threat	Aspect (C-I-A)[65]	Impact (H-M-L)	Likelihood (H-M-L)	Risk (H-M-L)	Response & Recommendation: Accept, Mitigate, or Transfer[66]
Big Mac hardware problem	I,A	H	L	H	Mitigate: • Back up data (5) • Archive old customer data (5) Transfer: Data recovery clause in business insurance
PC hardware problem	I,A	L	M	L	Mitigate: • No customer data on PC (5) • Back up system (5)
Staging hardware problem or virus	I,A	L	M	L	Accept
Macintosh virus	IA	H	L	H	Mitigate: • Harden the system (4) • Keep antivirus software up to date (4) • Back up data (5) • Archive old customer data (5) Transfer: Data recovery clause in business insurance
PC virus	I,A	L	L	L	Mitigate: • Harden the system (4) • Keep antivirus software up to date (4) • No customer data on PC (5)
Computers stolen in a break-in	A,C	H	L	H	Mitigate: • Physical security measures already in place (4) • Add cables to physically secure computers (4) • Back up data to safe location (2,5) • Archive old customer data & remove it from computers.(5) • Install MacPhoneHome & PCPhoneHome (7) Transfer: Business insurance.

[65] Confidentiality, Integrity, and Availability: what aspect of this asset is threatened?
[66] Numbers after Mitigation methods are Bass & Robichaux's risk responses (p.66): 1-avoidance, 2-transfer of assets, 3-reduce threat, 4-reduce vulnerability, 5-reduce criticality, 6-detection, 7-recovery. This is discussed in more detail in the "Assess responses to the risks" section.

Threat	Aspect (C-I-A)	Impact (H-M-L)	Likelihood (H-M-L)	Risk (H-M-L)	Response & Recommendation: Accept, Mitigate, or Transfer
Cracker "0wn1ng" Big Mac	CIA	H	L	H	Mitigate: • Harden the system (4) • Back up data (5) • Archive old customer data & remove it from Big Mac (5)
Cracker "0wn1ng" PC	CIA	M	M	M	Mitigate: • Harden the system (4) • No customer data on PC (5)
Electrical surge due to lightning or other cause	IA	H	L	H	Mitigate: • Back up data (5) • Use UPS's (4) Transfer: • Business insurance covers replacing dead computers • Data recovery clause in business insurance
iBook lost or stolen while traveling.	CA	H	M	H	Mitigate: • Back up data (5) • Archive old customer data & remove it from iBook. (5) • Install MacPhoneHome (7) Transfer: Business insurance.
Fire in office	A	H	L	H	Mitigate: • Back up data to safe location (2,5) • Smoke alarms & fire extinguishers (6,4) • Price a Halon fire control system (4) Transfer: Business insurance.
A cracker steals order information from the web server before it gets to the Business.	CIA	H	M	M	Mitigate: • File/directory security set up well on web server (4) • Orders never emailed with credit card numbers (5) Transfer: Liability clause in business insurance.
Cracker intercepts customer information over cordless phones	C	H	L	M	Transfer: Liability clause in business insurance.

Threat	Aspect (C-I-A)	Impact (H-M-L)	Likelihood (H-M-L)	Risk (H-M-L)	Response & Recommendation: Accept, Mitigate, or Transfer
Owner accidentally deletes old order files (human error)	IA	L	L	L	Mitigate: • Archive old customer data (5) • Back up data (5)
Cracker intercepts data over wireless network	C	H	L	M	Mitigate: Add WEP (4) Transfer: Liability clause in business insurance.
Order information is stolen from the Big Mac or the iBook by an employee and used for identity theft	CIA	H	L	M	Mitigate: • Few, well-screened employees (3) • Employees normally working under direct supervision (4) Transfer: Liability clause in business insurance.
A customer list (names and addresses) is printed by an employee and given to a competitor	C	M	L	L	Mitigate: • Few, well-screened employees (3) • Employees normally working under direct supervision (4) Transfer: Liability clause in business insurance.
Business is slandered by a competitor or former customer	I	M	L	L	Mitigate: Good communication with vendors and customers (4) Otherwise, Accept.
Orders go out late and customers are angered, taking business elsewhere.	IA	H	L	M	Mitigate: Owner works hard to set expectations properly and to get orders out on time (4,5). Otherwise, Accept.
A phone order is lost and never found, or found too late.	IA[67]	H	M-H*	H	Mitigate: Create half-page form, place near all Business phones. Form is placed directly on Orders clipboard when filled out (4).
An item advertised becomes no longer available to Business.	IA	M	M*	M	Mitigate: Good communication with vendors and customers (4)

[67] Integrity of the customer relationship and information; Availability of the information itself, and possibly of the relationship with that customer.

Threat	Aspect (C-I-A)	Impact (H-M-L)	Likelihood (H-M-L)	Risk (H-M-L)	Response & Recommendation: Accept, Mitigate, or Transfer
Misc. fixtures & equipment destroyed or damaged in fire or stolen in break-in	IA	M	L	M	Mitigate: Physical security measures already in place (4) Transfer: Business insurance.
Owner gets sick and is in hospital for a week	A	M	M*	M	Mitigate: • Owner taking care of herself in terms of health (4). • Husband learning technical details (5). Transfer: Investigate disability insurance.
Owner or staff is given and passes on bad information about stock	I	L	L	M	Mitigate: Owner reads and studies widely in the field, and staff defer to her on customers' technical questions (4).
Paper records stolen in break-in	CA	H	L	H	Mitigate: • Physical security measures already in place (4) • Lock all paper archives in a sturdy cabinet (preferably a fireproof safe) (4).
Stock stolen in break-in	A	H	L	H	Mitigate: • Physical security measures already in place (4) • Lock stock in locking file cabinets (4). Transfer: Business insurance.
Stock, paper records destroyed by fire in garage	A	H	L	H	Mitigate: • Smoke alarms & fire extinguishers (6,4) • Price a Halon fire control system (4) Transfer: Business insurance. Accept: • Increased vulnerability to credit card chargebacks • Replacement stock will take a week or more to arrive.

* This risk has affected the company before. It cannot, therefore, be considered Low risk unless significant precautions have been taken.

Threat	Aspect (C-I-A)	Impact (H-M-L)	Likelihood (H-M-L)	Risk (H-M-L)	Response & Recommendation: Accept, Mitigate, or Transfer
Stock, paper records destroyed by flood in garage	A	H	L	H	Transfer: Business insurance. Accept: • Increased vulnerability to credit card chargebacks • Replacement stock will take a week or more to arrive.
Website becomes unavailable due to hosting firm going out of business.	A	H	L	M	Mitigate: Complete copy of site on staging server exactly as it is in production (5).
Website becomes unavailable temporarily due to a DOS or other "Internet forces of nature"	A	M	M	M	Mitigate: Keep Business's site as secure as possible (4). Accept that there are things beyond the Business's control.
Website is defaced by a cracker.	IA	M	L	M	Mitigate: • Keep Business's site as secure as possible (4). • Complete copy of site on staging server exactly as it is in production (5).
All physical assets destroyed in an earthquake	A	H	L	L	Transfer: Business insurance.
All physical assets destroyed in an hurricane	A	H	L	L	Transfer: Business insurance.
All physical assets destroyed in an tornado	A	H	L	L	Transfer: Business insurance.

Appendix Seven: Prioritized Recommendation List Presented to Business Owner.

1. **Back up all the Business's important data**. This is part of industry best practices for any data that the organization cares about, as it greatly reduces the impact to information availability from hardware failures, viruses, crackers, and other miscellaneous causes. This tends, however, to "fall through the cracks" in home and small businesses, as this is a risk that appears minor until it "bites you."
2. **Archive old data.** Determine what old data should be archived, archive it to CD-ROM or other media, verify the archives, and put the media in a fireproof safe or safe-deposit box. Then remove the archived data from the computers. This not only reduces the impact of confidentiality and availability risks by a huge margin, but it also reduces the impact of integrity risks (the owner can go look up old data if she needs it, and know that it has not changed). A concern has recently been raised regarding the longevity of CD-ROM media, however, so the owner must be aware of this.[68]
3. **Harden computer systems and the network according to best practices**. I have documented the system audits and specific recommendations for each computer and the router in Appendices 2 through five.
4. **Protect stock and paper records with a fireproof lockbox or equivalent.** The stock and paper records were vulnerable to both fire and break-ins, and they were just sitting there on the shelf. While both of these risks were low likelihood, the impact of simultaneously losing the stock and previous years' business records would be very high. A large enough fireproof lockbox for the stock, however, was not cost-effective, and the Business owner chose not to implement this recommendation.
5. **Physical defense in depth for the computers.** The computers are in a room with a locked door, but with windows. There are industry-standard cables manufactured for securing computers and the cases of all of the Business's computers already had niches to accept them.
6. **Create a half-page form for phone orders and place copies near all Business phones.** This form, printed on colored paper, should help prevent phone orders from being lost in the shuffle. A copy has been reproduced below.
7. **Price a halon-based fire control system.** This, not surprisingly, turned out to way out of the Business's price range, but we had to evaluate options. These systems, typically seen in professional-grade data centers, can put fires out without the danger to computers represented by water.

[68] Libbenga. This English-language article references a scientific study in Dutch that I have been unable to translate, so I am forced to rely upon Libbenga's English-language summary.

PHONE ORDER

Name:_____ Phone:_____

Shipping Address:_____
City, State, Zip:_____

Billing Address:_____
City, State, Zip:_____

Email Address: _____

Order: _____ _____ _____

_____ _____ _____

Credit Card: VISA MASTERCARD DISCOVER

Card #: _____ CVV Code:_____ Exp. Date: _____

Shipping Instructions: