D Appendix D: Convenience Vs. Security:

Case Significance

The security practices of Book Box give significant insight into cybersecurity management because the choices made by the CISO demonstrate the need to balance customer protection with customer satisfaction. Convenience versus security is a typical challenge that CISO's must overcome when protecting the information of online customers.

Summary of Conclusions

- **A CISO must make trade-offs and remian within their budget, while still optimizing customer protection.**
- **Balancing the ability to protect the customer, with the need to retain their business is a necessary challenge for CISO's.**
- **Simply buying the most expensive security features does not guarentee that customers will remain satisfied**

The Cost-Benefit Analysis of the Book Box Website Security Practices

Established in 2003, Book Box is a popular online retailer that sells new and used books. The company exclusively sells their products over the Internet. Book Box operates a secure website and their customers are confident in the company's ability to protect their personal information, including credit card information. However, due to the large volume of transactions done on this online superstore, the Book Box website is still vulnerable to being hacked by cyber criminals. Despite the fact that Book Box has been doing great business for many years, their customers trust them, and they are the largest online book retailer on the web, a data breach could still irreparably harm their reputation. If a hacker were able to successfully steal customer information, the consequences for the company could be devastating. Such an incident could allow Book Box's competition to acquire the customers that no longer trust the site. Moreover, such a data breach could even result in a lawsuit against Book Box. If it could be proven that the company did not take the steps necessary to protect their customers personal information, Book Box could be found liable for losses.

In order to prevent the possible catastrophic consequences of a hacking incident, Book Box decides to redouble their efforts to protect their website. The Chief Information Security Officer (CISO) orders a Risk Assessment to be done immediately.

Company Profile

Established in 2003, Book Box is a popular online retailer that sells new and used books. The company exclusively sells their products over the Internet on their secure website. Within the online book selling market, their customers are confident in the company's ability to protect their personal information, including credit card information. Book Box has never been hacked, nor have they had any other security breach involving sensitive customer data. While not number one in online book sales, the company enjoys healthy profits and high customer satisfaction.

Online Book Seller Environment

Despite the fact that online shopping is as common today as is shopping at brick and mortar stores, customers who shop online are still taking a risk in doing so. Whenever a customer enters their credit card number or bank account number into an online form, she is exposing herself to the potential dangers lurking on the web. Most sites are secure, and all reputable retailers use security controls to ensure that their customers are safe from online predators. However, many well-established and well-intentioned online retailers have been hacked over the past few years, which resulted in financial damages, government inquiries and penalties, and customer distrust.

Just six months ago Read All About It, another online book seller and a close competitor to Book Box, suffered a security breach on their site. The website was hacked and hundreds of customer credit card numbers were stolen. The security of customer names, phone numbers, and billing addresses was also breached. Read All About It is a reputable company with a large customer following. In the wake of the breach, the company faced media scrutiny, customer outrage, lawsuits, and government interventions. While the company had worked for many years to establish themselves as a legitimate online retailer, one security breach might have set them back to square one. It is unlikely that Read All About It will ever fully recover from the cybersecurity breach. Their reputation is now shaky, and they lost both money and their competitive edge in the wake of the breach. Furthermore, the Read All About It incident has led to a far more cautious online consumer base.

Customers of online retailers - and particularly those like Book Box and Read All About It who store sensitive customer information on their sites - are demanding higher security standards from book sellers. Along with this desire for better website security controls, customers still want a convenient and fast shopping experience. This ideal shopping experience fits in with the overall expectations of the online shopping environment. Most people want to have the convenience of a one-button checkout, and the option of having their username and/or password saved in their Internet browser. Customers are put off by strict password strength guidelines and multi-factor authentication procedures.

This means that the average Book Box customer would rather create a password that is personal and easy to remember than one that includes numbers, capitalized letters, symbols, and a minimum length of characters. Similarly, the average Book Box customer does not want to go through an authentication process every time he logs in to buy a book. A customer does not want to answer security questions in addition to inputting his password, nor does he want to go through the process of entering his billing and credit card information as a guest every time he makes a purchase from the site. In an online retail environment in which convenience and security cannot necessarily coexist, and in which marketplace competition makes the alienation of customers disastrous for the bottom line, how does Book Box settle the apparent paradox of keeping their customers both happy and secure?

In the online book store environment, Chief Information Officers (CIO's) and Chief Information Security Officers (CISO's) are often charged with gathering the appropriate information regarding risk, presenting their findings, and working with the Board of Directors and other executive officers to solve the problem of convenience versus security. The problem of satisfying the preferences of online consumers while also effectively managing the risk to sensitive customer information is not an easy task. Managing risk means making tradeoffs, and often answering questions that do not actually have a right or wrong answer. Perhaps most importantly, risk management is limited by budgetary constraints.

Case Study

Given the current threat environment, the CISO of Book Box needs an answer to the question, "Which security controls are the best at protecting customer information from being leaked, and within our security budget, and will not inconvenience customers?" On the Book Box website, sensitive information has to be protected through at least three security measures:

Necessary Security Controls

1. Credit card details supplied by the customer, either to the merchant or payment gateway. Handled by the server's SSL and the merchant/server's digital certificates.
2. Credit card details passed to the bank for processing. Handled by the complex security measures of the payment gateway.
3. Order and customer details supplied to the merchant, either directly or from the payment gateway/credit card processing company. Handled by SSL, server security, digital certificates (and payment gateway sometimes).

In order to protect sensitive customer information, Book Box has existing security controls to which any new security measures will be added.

Existing Security Controls

- User ID and Password: Customers login to their Book Box account using an ID and password.
- SSL Certificates: A Secure Sockets Layer (SSL) Certificate encrypts credit card numbers.
- Secure shopping cart software: The shopping cart is secured by third party software.

The question of additional security protections is not merely answered by guessing. A rigorous mathematical process called a Risk Assessment is performed by experts in order to determine how the company ought to improve their cybersecurity posture. Even after the risk assessment is complete, and the CISO has gone over the findings, the Board of Directors must also review the results and finalize any decision made by the CISO. Thus, the CISO has a risk analyst perform a Risk Assessment, the results of which will determine which security features the CISO will choose from.

The Risk Assessment is finished and the risk analyst reports her findings to the CISO (review the Appendix for a detailed example of a Risk Assessment). The risk analyst presents the CISO with a list of security controls, all of which would aptly bolster the security of their website, and further protect their customers. However, the choice of which new security controls to implement is not so simple for several reasons.

First, the CISO has been allotted a budget of $100,000 to purchase additional security features. This means that she may have to sacrifice certain controls, or combinations of controls, that are outside of her budget. Second, each control has been assigned a number score relating to both customer protection and customer inconvenience. The CISO must keep the customer protection score above 8, and keep the customer inconvenience score below 9. The budgetary constraints, coupled with the protection and inconvenience criteria make the CISO's decision quite difficult. Furthermore, the blame for a failure in security or for losing customers due to inconvenience will rest on the CISO's shoulders. The following chart is presented to the CISO for review:

Additional Security Options

Security Feature	Cost	Customer Protection (5 being best)	Customer Inconvenience (5 being worst)
Multiple logins: In addition to logging into his account when he enters the site, the customer must confirm his username and password again before he can continue on to his shopping cart.	$20,000	2	2
Enhanced Password Strength: Each customer must include a capital letter, and at least one number or symbol in their password. This password must also be a minimum of eight characters.	$40,000	3	3
Address verification: Book Box must verify a customers address if there are any discrepancies from the address listed on the account from either the shipping or billing address entered in the checkout transaction. If there is a difference between the address that a customer has on file with their bank, or has used to register for their Book Box account, the transaction will be halted and an email notice will be sent to the customer, directing them to contact Book Box customer service.	$60,000	5	4
Card Verification Value: Customers must enter the 3 digit number located on the back of their credit card in order for the transaction to go through.	$80,000	5	2

Security Feature	Cost	Customer Protection (5 being best)	Customer Inconvenience (5 being worst)
Challenge Questions: During log-in, the system requires users to select three challenge questions and responses. If the risk score associated with a particular transaction exceeds 750, the challenge questions are be triggered. If the challenge question responses entered by the user do not match the ones originally provided, the customer receives an error message. If the customer is unable to answer the challenge questions in three attempts, the customer is blocked from his or her account.	$30,000	4	4
Dollar Amount Rule: The system permits Book Box to set a dollar threshold amount above which a transaction automatically triggers the challenge questions even if the user ID, password, and device cookie are all valid. Book Box set this dollar amount threshold at $250 per transaction.	$10,000	3	2

Security Feature	Cost	Customer Protection (5 being best)	Customer Inconvenience (5 being worst)
Invisible Device Authentication: The system places a "device cookie" onto customers' computers to identify particular computers used to access their account. The device cookie is used to help establish a secure communication session with the server. When the cookie is changed, the system asks a security question to verify that the correct user is logging in.	$70,000	4	1
Risk Profiling: The system entailed the building of a risk profile for each customer based on the location from which a user logged in, when and how often a user logged in, what a user did while on the system, and the size, type, and frequency of transactions. The Book Box security system records the IP address that the customer typically uses to log into online banking and adds it to the customer profile. If a user's transaction differs from its normal profile, the security system flags the transaction. Transactions generating risk scores in excess of 750, on a scale from 0 to 1,000, are high-risk transactions. High scores trigger the security questions.	$60,000	5	4

Analysis

The security controls above offer the CISO with many possible combinations, while still keeping her customer protection score above 8 and her customer inconvenience score below 9. The following chart shows two possible combinations that the CISO might choose.

Option 1

Security Feature	Cost	Customer Protection	Customer Inconvenience
Card Verification Value	$80,000	5	2
Multiple Logins	$20,000	2	2
Total	$100,000	7	4

Option 2

Security Feature	Cost	Customer Protection	Customer Inconvenience
Dollar Amount Rule	$10,000	3	2
Challenge Questions	$30,000	4	4
Risk Profiling	$60,000	4	2
Total	$60,000	11	8

If she chooses Option 1, the CISO would spend her entire budget on Card Verification Value and Multiple Logins. While she would have a great customer inconvenience score of 4, well under the threshold of below 9, her customer protection score would not reach the minimum expectation of being over 8. She could still choose to present this option to the Board, however they would likely want more customer protection for the $100,000 price tag.

If the CISO chooses Option 2 she would come in on budget with three new security controls. The customer protection score would be well over the target, thus making the features a good addition to their website. The customer inconvenience score would also remain just at their target. While this Option is good, and perhaps better for the company than Option 1, it is still possible that the Board may not be willing to risk such a high customer inconvenience score.

By analyzing all of the options, some important questions are raised. What are the pros and cons of each additional security measure that she chose? Will enhanced security features like the multiple logins alienate the customers too much? Is it worth allowing for more convenience, yet leaving customers with a less secured shopping experience? Furthermore, what less obvious impacts might new security controls have on the company? For example, will Book Box be able to properly train employees to complete the Risk Profiling? Will they have to hire new employees to complete and/or oversee that task? These questions demonstrate that the job of the CISO is not easy, and that the job of managing risk and securing products and services is complicated.

Conclusion

Many factors go into choosing the best security options for securing an e-commerce website. Customer protection and convenience are important, yet every company has different needs unique to their business model, software, budget, personnel, etc. The challenge of maintaining customer privacy, securing customer data, and ensuring that customers are not alienated by too many security features is daunting. In order balance all of these fragile factors, a CISO of an online retailer must be an excellent manager. This means that she must be able to think through problems, recognize and understand budgetary constraints, be able to look ahead and predict potential problems, understand risks and rewards, answer questions that do not have a right or wrong answer, and have the ability to make trade-offs and compromise when necessary. Perhaps most importantly, the CISO of an online retailer must understand how to balance customer protection with customer convenience.

Appendix

Example Research Model

Book Box wants to find affordable security controls that are appropriate for reducing the risk of customer information being leaked. To evaluate this question, the risk analyst will use a statistical regression model. As described in Chapter 2.6 of Cybersecurity Fundamentals, a regression model uses multiple independent (x) variables to predict or estimate a dependent (y) variable. Presumably, a change to any of the independent variables will affect the outcome(s) of the model. In other words, the y-value is dependent on the x-value(s). In the case of multivariable analysis, each x-value must be mutually exclusive; the x-values cannot be affected by, nor dependent upon, each other.

In order to determine which security controls are the best at protecting information, the risk analyst will survey 200 (n=200) other online retailers. Using 'yes' or 'no' answers, the retailers will respond to the question of whether or not customer information was leaked on one random day (24 hours) in 2011.

Because the risk analyst is dealing with a yes or no question (also called a binary question), she will use a logistic (logit) regression model to evaluate risk. Logit models are used when the dependent variable is a binary response. The model generates a probability value. A logit model reveals (1) the most statistically significant indicators and (2) the type of association the indicators form with the dependent variable - a positive (direct) or a negative (indirect) relationship. A positive relationship indicates that if the independent variable increases, the dependent variable increases; a negative relationship means if the independent variable decreases, the dependent variable acts in the opposite manner, so in this case the dependent variable would increase.

Example Analysis of the Most Significant Factors Influencing Customer Information Leaked

Based on the most complete model generated using the logit equation, Strength of Password and a 2-Factor Authentication are the two most significant security controls. An example of a strong password includes capitalization, a number, a symbol, and at least eight characters, unrelated to any personal information, such as "rh7TL!9". The simplest type of password is a word that is found in a dictionary, such as the word "password". A 2-Factor Authentication is a pair of security controls that requires the user to enter either 1) "something the user knows", such as a password, 2) "something the user has'", such as an account number, and/or 3) "something the user is", such as a biometric data. 2-Factor Authentication is the most significant variable based on its low p-values in all three models.

According to the logit analyses, the independent variable Password is significant in determining the probability of a risk (defined as customer information being leaked), and as the password becomes stronger by gaining in complexity, it becomes less likely that customer critical information will be leaked.

Example of Predicting the Probability of Customer Information Leaked

The strength of multivariate statistical analysis lies in its predictive capabilities. A thorough, valid, and reliable design will allow a risk manager to extrapolate future trends that will help Book Box protect its customer's sensitive information.

Recall that the best security controls for protecting customer information are a strong Password and a 2-Factor Authentication. However, the risk analysis team wants to know the combination of security controls

that will best protect customer information from malicious code, based on the resources allocated and constraints placed on Book Box.

Model A is the riskiest scenario: There is a 93.136% likelihood of customer information being leaked under the set of conditions. Model D is the safest and most realistic option, which even takes into consideration a hacker with strength level 7 out of 10, 10 being the strongest.

Model D is the only model that has a 2-Factor Authentication and it has the strongest password. While Model D does contain multiple security controls, it is a realistic option. Consumers may not enjoy having a 2-Factor Authentication; however, on a popular website that is a target for strong and capable hackers, consumers should feel confident that there is only a 0.641% likelihood that their critical information may be leaked.

Example of Findings

The most significant independent variable is the presence or lack of presence of a 2-Factor Authentication. Therefore, if a 2-Factor Authentication is present as a security control on a company's website, then the likelihood of customer information being leaked decreases. According to this analysis, and based on its statistical significance in each model, 2-Factor Authentication is the most significant form of security control that the online retailer can use to reduce the likelihood of customer information being leaked.

Based on these models, the risk manager may suggest to the Book Box CISO that the website requires a strong password and a 2-Factor Authentication in order to secure customer information. Decisions made in these areas should be based on an effective risk management program. However, the CISO has limited resources for the deployment of security controls, so she must choose a combination of controls that securely safeguards customer information, avoids customer inconvenience, and works for the company's budget. At this point, a cost-benefit analysis is necessary to determine which controls should be in place.

Following our risk determination process in this example, the CISO now has four different models to present to the Board of Directors as reasons to promote the security controls of Model D versus Model A. The CISO will emphasize the need for 2-Factor Authentication and a strong Password for customer login.