Tyler Jackson

2/12/2015

Risk Assessment Report

Company: Must Love Dogs Inc.

I. Introduction

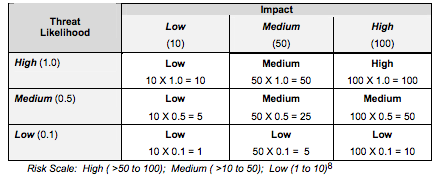
The purpose of this risk assessment is to provide the owner of Must Love Dogs Inc. with the means to view, analyze, and mitigate its various risks. This report will include an in-depth look at the company’s assets. threats, and vulnerabilities. The company is a boarding kennel for dogs. The employees include managers as well as kennel technicians. The various assets range from the land to the cost for paper towels. We also include components such as customers, reputations, and industry relationships.

II. Risk Assessment Approach

The assessment was conducted by Tyler Jackson through a few different methods. Mainly, the techniques used were brainstorming, industry research, and an interview with the owner. The interview was conducted last in order to verify the results, and create a more comprehensive report. I determined the risk using a 3x3 risk-level matrix. This risk is calculated using the threat likelihood which is either .1, .5, or 1 and the impact on the company if the threat is exploited which is either low (10), medium (50), or high (100). In order to get the risk you multiple the threat likelihood by the impact. I chose to use a 3x3 matrix because the complexity of the risks for this company are relatively low. If there were a high number of risks and they were complex then it would be important to have a more specific risk-level matrix, but for Must Love Dogs the 3x3 risk-level is enough.

Table II.I

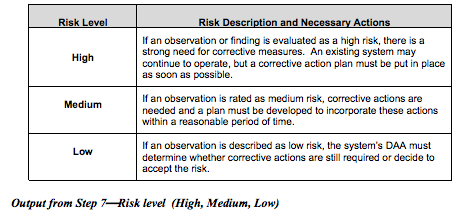
Risk-Level Matrix



The table below was taken from NIST Risk Management Guide and describes the various descriptions of each risk level.

Table II.II

Risk Scale and Necessary Actions



III. System Characterization

Characterize the system, including hardware (server, router, switch), software (e.g., application, operating system, protocol), system interfaces (e.g., communication link), data, and users. Provide connectivity diagram or system input and output flowchart to delineate the scope of this risk assessment effort.

Table III.I

System Characterization

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Assets** | **Asset Attributes** | **Asset Valuation ($-$$$$$)** | | | |
|  |  | Critical To Success | Generates Revenue/Profit | Expense to Replace | Most Embarrassing if Revealed/Greatest Liability |
| Employees | -Experience | $-$$$$$ | $-$$$$$ | $-$$$$$ | $$$ |
|  | -Training |  |  |  |  |
|  | -Certifications |  |  |  |  |
|  | -Performance History |  |  |  |  |
|  | -Salary/Benefits |  |  |  |  |
|  | -Accessibility |  |  |  |  |
|  | -Licenses |  |  |  |  |
|  | -Supervisor |  |  |  |  |
|  |  |  |  |  |  |
| Customers | -Loyalty | $$$$$ | $$$$$ | $$$ | $-$$$ |
|  | -Regularity |  |  |  |  |
|  | -Spending Habits |  |  |  |  |
|  |  |  |  |  |  |
| Cleaning Equipment | -Difficulty to Store | $$$$$ | $$$$ | $-$$$ | $$ |
|  | -Ease of Use/Labor Intensive |  |  |  |  |
|  | -Frequency of Use |  |  |  |  |
|  | -Effectiveness |  |  |  |  |
|  | -Durability |  |  |  |  |
|  |  |  |  |  |  |
| Building | -Size | $$$$$ | $$$$ | $$$$$ | $ |
|  | -Durability |  |  |  |  |
|  | -Facilities |  |  |  |  |
|  | -Runs (Quality/Quantity) |  |  |  |  |
|  | -Age |  |  |  |  |
|  | -Security |  |  |  |  |
|  |  |  |  |  |  |
| **Assets** | **Asset Attributes** | **Asset Valuation ($-$$$$$)** | | | |
| Property | -Location | $$$$$ | $$$ | $$$$$ | $ |
|  | -Terrain |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Cash | -accessibility | $ | $ | $ | $ |
|  | -amount |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Supplies - Feeding | -Durability | $$$$$ | $$$$ | $$ | $ |
| - Cleaning | -Life Expectancy |  |  |  |  |
| - Runs | -Quantity |  |  |  |  |
| - Activities | -Size |  |  |  |  |
| - Office | -Quality |  |  |  |  |
|  | -Frequency of Use |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Business Model | -Marketing Strategies | $$$$$ | $$$$$ | $ | $ |
|  | -Cost Structure |  |  |  |  |
|  | -Upcharges |  |  |  |  |
|  | -Seasonal Discounts |  |  |  |  |
|  |  |  |  |  |  |
| Social Media Pages | -Exposure | $$$ | $$ | $ | $$$$$ |
|  | -Type (FB, Insta, Twitt) |  |  |  |  |
|  | -Quality |  |  |  |  |
|  | -Effectiveness |  |  |  |  |
|  |  |  |  |  |  |
| Computers | -OS | $$$ | $$$ | $$ | $$ |
|  | -Model |  |  |  |  |
|  | -Quantity |  |  |  |  |
|  | -Frequency of Use |  |  |  |  |
|  | -Companywide Popularity |  |  |  |  |
|  |  |  |  |  |  |
| Cameras | -Quality (Resolution, Distance, Range, etc.) | $$$ | $$ | $$$ | $ |
|  | -Placement |  |  |  |  |
|  | -Type (Audio, Video, Infrared, etc.) |  |  |  |  |
|  | -Purpose |  |  |  |  |
|  | -Effectiveness |  |  |  |  |
|  |  |  |  |  |  |
| **Assets** | **Asset Attributes** | **Asset Valuation ($-$$$$$)** | | | |
| Reputation | -Customer Satisfaction | $$$$$ | $$$$$ | $$$$$ | $$$$$ |
|  | -Puppy Satisfaction |  |  |  |  |
|  | -Quality of Service |  |  |  |  |
|  | -Cost/Reward |  |  |  |  |
|  | -Employee Likeability |  |  |  |  |
|  | -Business Ethics |  |  |  |  |
|  |  |  |  |  |  |
| Website | -Size | $$$ | $$$ | $$ | $$ |
|  | -Data Input/Output |  |  |  |  |
|  | -Encryption Protocols |  |  |  |  |
|  | -Purpose |  |  |  |  |
|  | -Accessibility |  |  |  |  |
|  | -Authentication Protocols |  |  |  |  |
|  |  |  |  |  |  |
| Procedures and Policies | -Owner | $$$$$ | $ | $$ | $$$$$ |
| -Cleaning | -Inputs & Outputs |  |  |  |  |
| -Injured Animal | -Influence |  |  |  |  |
| -Injured Employee | -Efficiency |  |  |  |  |
| -Write Up Policies | -Expected Results |  |  |  |  |
| -Termination |  |  |  |  |  |
| -Day Care |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Applications | -Security | $$$$$ | $$$$$ | $ | $$ |
|  | -Ease of Use |  |  |  |  |
|  | -Frequency of Use |  |  |  |  |
|  | -Purpose |  |  |  |  |
|  | -Support |  |  |  |  |
|  | -Platform |  |  |  |  |
|  |  |  |  |  |  |
| Televisions | -Quality | $$ | $$ | $$$ | $ |
|  | -Quantity |  |  |  |  |
|  | -Model |  |  |  |  |
|  | -Placement |  |  |  |  |
|  | -Purpose |  |  |  |  |
|  |  |  |  |  |  |
| **Assets** | **Asset Attributes** | **Asset Valuation ($-$$$$$)** | | | |
| Physical Security System | -Provider | $$$$ | $ | $$ | $$$$$ |
|  | -Components |  |  |  |  |
|  | -Frequency of Use |  |  |  |  |
|  | -Ease of Use |  |  |  |  |
|  | -Purpose |  |  |  |  |
|  | -Components |  |  |  |  |
|  |  |  |  |  |  |
| Shuttle | -Model | $$$$ | $$$$ | $$$ | $ |
|  | -Make |  |  |  |  |
|  | -Insurance |  |  |  |  |
|  | -Size |  |  |  |  |
|  |  |  |  |  |  |
| Company Policies | -Influence | $$$ | $ | $ | $ |
|  | -Strictness |  |  |  |  |
|  | -Effectiveness |  |  |  |  |
|  | -Purpose |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Data | -Where is it stored | $$$$$ | $$$ | $ | $$$$$ |
| -Financial Records | -What is Stored |  |  |  |  |
| -Customer Information | -How is it stored |  |  |  |  |
|  | -Accessibility |  |  |  |  |
|  | -Insurance |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Industry Relationships | -Who/What | $$$$ | $ | $$$ | $$$$$ |
| -Food vendors | -Purpose |  |  |  |  |
| -Dog Trainers | -Age |  |  |  |  |
| -Veterinarians | -Frequency of Use |  |  |  |  |
| -Reporters | -Quality |  |  |  |  |
| -Agricultural Department |  |  |  |  |  |

IV. Threat Statement

Table IV.I

Threat Source, Motivation, and Action

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Threat Source** | **Motivation** | **Threat Action** |
| Disgruntled Employee | -Revenge | -Go to the press |
|  | -Money | -Law Suit |
|  | -Fame | -Sabotage the Company |
|  |  | -Steal an animal |
|  |  | -Hurt another employee |
|  |  | Steal Cash |
| Competitor | -Decrease the Competition | -Slander Must Love Dogs |
|  |  | -Steal their client lists |
|  |  | -Steal Business Model |
|  |  | -Steal Procedures |
| Natural Disaster | -No Motivation | -Tornados |
|  |  | -Floods |
|  |  | -Brush Fires |
|  |  | -Lightning Damage |
| Robber/Thief | -Get Money | -Break in and steal cash |
|  | -Get a Dog | -Break in and Steal a Dog |
| **Threat Source** | **Motivation** | **Threat Action** |
| Unhappy Guest | -Revenge | -Slander on Business Review Sites |
|  | -Get Money | -Slander on Social Media |
|  |  | -Slander to the Press |
|  |  | -Slander to the News |
|  |  | -Law Suit |
|  |  | -Steal Money |
|  |  | -Sabotage the Company |
| Lawyers | -Money | -Sue from Guest |
|  |  | -Sue from Employee |
| Newspaper/Media/Social Media | -Get a Good Story | -Slander the Company |
|  |  | -Run a story containing Slander by Guest or Employee |
| Power Failure | -No Motivation | -Electricity Goes Out |
| Market Fluctuations | -No Motivation | -People Travel Less |
|  |  | -People Take Less Vacations |
|  |  | -Less People Work (Less Day Care) |
| Kennel Cough | -No Motivation | -Animals Get Sick (less animals stay at kennel) |

V. Risk Assessment Results

Table V.I

Vulnerability/Threat Pairs

|  |  |  |  |
| --- | --- | --- | --- |
| **Observation #** | **Vulnerability** | **Threat Source** | **Threat Action** |
| 1 | No Public Relations Team to monitor social media platforms. | Disgruntled Employee | Slander the Company on Social Media |
|  |  | Unhappy Customer |  |
| 2 | Back up plan for computers malfunctioning is writing financial information down. | Thief/Robber, Unhappy Customer | Steal the financial information (Credit Card #s, addresses, contact information) |
| 3 | A user's login credentials don't expire upon termination. | Disgruntled Employee | Login to the computer and gain access to company information after being terminated |
| 4 | Manager's Office Is Not Locked | Disgruntled Employee | Could steal video surveillance and/or Logged Complaints |
| 5 | Poor Physical Security | Thief/Robber, Unhappy Customer | It is relatively easy to walk in and take a dog with the only line of defense being an employee.  Break in and steal from the cars. |

Next we will discuss the risk of these various observations.

Observation 1:

There is no public relations team or system in place to monitor media platforms for bad press about the company. The actors that pose a threat to this vulnerability are anyone who might want to cause harm to the company. This could range from a disgruntled employee to an unhappy guest, to a competitor. The threat action would be to post anything slanderous towards Must Love Dogs on a media platform. Any form of social media, a newspaper article, or a televised news broadcast would fall under this category. There are also business review websites that one could post slanderous remarks on in order to hurt the company. The likelihood of this threat is marked as high (1) for a few reasons. It is very easy to post things on media platforms in this day and age with generally no consequences making people more likely to do it. This has also happened in the past making the odds of it happening again stronger. The impact of this kind of threat is also very high (100). This threat would affect a few different assets, most importantly being Customers and Reputation. If you refer back to the System Characterization (Table III.I) you can see that these two assets are extremely critical to success, and also generate a large amount of revenue. If the likelihood is multiplied by the impact, (1 \* 100) there is a risk level of High (100). This can be confirmed by referring to Table II.I. One existing security mitigation control for this threat is an employee whose job is to maintain and manage social media platforms for the company. This person could theoretically try to counter any negative press with positive press, but a preferable system would include a team of public relation professionals whose job it is to monitor media platforms for bad press and to determine game plans to spin all press into a positive light. As this risk is rated as High, it would be highly recommended to have some form of public relations management in the case of an attack to the company via the media. A large monthly flat fee may seem like an extra unnecessary cost, but when compared to potentially $100,000s of loss from the result of reputation attacks it is worth it.

Observation 2:

The back-up plan for if the computer systems go down is to write the customers’ financial information down. This would consist of writing credit card numbers with names and phone numbers down on a legal pad that is kept next to the computers at the reception desk. The actors that pose a threat to this vulnerability are any thief, or unhappy customer. Unless someone is constantly monitoring the front desk area it would be relatively easy to lean over the counter and copy a few credit card numbers down at a time. The threat action would therefore be stealing financial information. The likelihood of this threat is relatively low (.1), because of the type of people that come into the kennel. It is not a likely target for petty thieves, and someone would have to know the system intimately in order to know about the vulnerability making it less likely to be exploited. The impact of a threat like this would be relatively high (100) because it would not only affect the Data asset, but also the customer and reputation asset. If customers found out that the company leaked financial information their reputation would take a serious blow. Therefore, the risk level would be Low (10) which is calculated from 100 \* (.1). Currently the main security mitigation in place to prevent this threat is security cameras that are on the front desk at all times. While this isn’t a preventive security measure, it will function as a deterrent. The risk level is low for this operation, so it is up to the company to decide if purchasing a second set of computers to be used in case the first goes down would be worth it. Another option could be to purchase support for the applications the company uses in case they go down. In theory, the purchased support would lead to faster recovery times.

Observation 3:

An employee’s login credentials don’t expire upon login which is a vulnerability in the software of the company. The threat actors that could exploit this vulnerability are terminated employers who might want to cause harm to the company. The threat actions would be to come into the business, login to the computer when your authorization should have been revoked and obtain company information. This information could be financial information, or reservation information which could be very valuable to sell to a competitor. The likelihood of this threat is low (.1) for a couple reasons. One, you would have to come into the company when no one was at the receptionist desk, and two you would have to avoid getting caught on camera. The impact of this threat would be relatively low (10) as well, because the guests credit card information is not stored on the local computers, and every employee who accesses the financial information has to authenticate. This deters any employee from attempting this kind of action. Therefore, the risk level of this threat is low (1) calculated from 10\*(.1). Currently the security mitigation controls in place are the cameras in the front office area that overlook the computers. Although this is has a low risk level, the fix is so inexpensive that it is strongly recommended. All that would be required is to delete the terminated employee’s authentication credentials from where they are being stored. Deleting their credentials would be free and easy.

Observation 4:

The manager’s office is not locked 24/7. The threat sources for this observation range from a thief, to a disgruntled employee, to an unhappy guest. The threat actions would be to break into the action and steal employee information, or surveillance footage. The likelihood of this are medium (.5) because it would be very easy to do, but not very necessary. For example, for someone to get caught another employee would have to see them, or a manager would have to see them. Another possibility is that a manager reviews the surveillance footage and catches them going in/out of the office. Even if one were to see an employee in the office, it would most likely not be viewed as out of the ordinary. The reason it is not very likely is because the documents and footage in the office are not very confidential. The impact of this threat would be low (10), because while the threat impacts employees, the impact it would have is relatively small. The risk level is therefore medium (50) calculated by 10\*(.5). The current security mitigation controls for this observation are the fact that managers are usually in the office, or near the office which would make the risk for the threat actors higher. There are also cameras in front of one of the entrances. This has a medium security risk level and therefore needs a plan for a correcting protocol in place. One cheap fix would be to install doors with a lock. The doors could remain open when a manager was inside the office, but would be shut and locked every time they left. This would be an easy and cheap fix, but would have the potential for becoming very tedious to the managers. Another solution would be to put cameras in the office, and to keep the employee information and surveillance equipment in locked cabinets.

Observation 5:

There is poor physical security around the company meaning it is generally just a lock that is separating the dogs and employees from a thief or robber. There are video cameras placed all around the building as well, but these are not reviewed regularly enough to be useful unless someone notices something is stolen. For example, if a theft went unnoticed for a month it is possible it would get buried amongst surveillance footage. There is also a parking lot on the property that has no real physical security other than a 6 foot tall gate. The threat sources in this observation are therefore thieves. The threat actions would consist of breaking into cars in the parking lot, or into the building. Once in the building a thief could attempt to steal cash, supplies, or even an animal in the worst case scenario. It also poses a threat to the employees who would be working at the time. It is a 24-hour facility, so it becomes increasingly important to have strong security at the odd hours of the night. The likelihood of this threat are low (.1) because of the cameras, and fact that someone is on the property 24 hours a day. The impact would be very high (100) if the theft was a dog, or some sort of harassment to an employee. If a dog was stolen, the reputation would take a huge blow, the customer base would diminish to an extent, and there would be a very strong possibility of backlash via media platforms. The risk level would be low (1) in the case of a vehicle break in calculated from 10\*(.1). In the case that someone breaks in and harasses an employee or steals a dog the risk would be low (10) again calculated from 100\*(.1). The current security mitigation controls in place for this threat are the cameras placed strategically around the building and the locks on the outside of the building. While the footage isn’t monitored daily, it will still function as a deterrent. One possible fix would be to hire a nighttime security officer to monitor the security cameras and patrol the property. This would be a significant extra cost however for a low level risk.

VI. Summary

There were 5 total observations with 3 low risk levels, 1 medium, and 1 high. The low risk level observations all have relatively cheap and easy fixes. The high risk level observation has an expensive fix, but is highly recommended. The observation with medium level risk is the one where a decision needs to be made. The risk level is medium, so correctional changes are recommended but do not need to be implemented immediately.

|  |  |  |  |
| --- | --- | --- | --- |
| **Observation #** | **Risk Level** | **Reccomendations** | **Comments** |
| 1 | High | -Hire some sort of PR representation | -This will be expensive, but try to weigh the lost revenue from a huge hit to the company's reputation against the cost of hiring the PR team. |
| 2 | Low | -Purchase a back up set of computers. | -Remember this is low risk, so if you are strapped for cash it is not urgent. That being said, if you have the cash to fix it you should because it is relatively inexpensive. |
|  |  | -Purchase software support. |  |
| 3 | Low | -Delete user credentials upon termination | -Although this is a low risk observation the fix is free and therefore strongly recommended. |
| 4 | Medium | -Install locks on office doors and keep door closed at all times if a manager is not in the office. | -This is an easy fix, but could become tedious and interrupt the workflow of the day. |
| 5 | Low | -Review security cameras more often. | -Hiring an officer would be preferable, but is an expensive fix for a low level risk. |
|  |  | -Hire a nighttime security officer. |  |