**SRA311**
**Fall 2010**

# UrRisk#04

Table#01

Ryan Glynn/RDG5060

Josh Shtatman/JAS5662

# Introduction

This risk assessment suggests what the Nittany Lion Inn should do to improve the security of the hotel lobby in terms of financial risks from their computer system and theft. Due to time constraints, the assessment is limited to only the financial risks, all other types of risks and the reasons why they were not chosen are stated within the scope section of this assessment.

Within the assessment section, our methodology and reasoning for this methodology are stated in the "Risk Assessment Approach" sub-section. Under "System Characterization" we state that inputs, outputs and processes of the Nittany Lion Inn. These items are continued into the "Threat Statement" and the possible issues that are caused by the processes and inputs are then stated. The results are then stated and discussed along with the suggested actions to improve these risks all within the sub-section "Risk Assessment Methods and Results". The full process and assessment is then summarized within the conclusion sub-section.

## *Purpose*

The purpose of this risk assessment is to provide hotel management with information concerning possible risks within the hotel lobby that may cause a loss in the hotel's overall financial assets. The reasoning for such a specific scope is due to the amount of larceny reported in State College is double the national average (see Attachment 1 for full details). Property crime is also as high as the national average, which makes these two issues the top priority for businesses in the State College area.

## *Scope*

Items that are to be assessed include financial risks caused from abuse or misuse of Nittany Lion Inn lobby computers as well as theft and destruction of hotel property. Theft of hotel property, including small items such as candy bars from the lobby, can gradually add up to a significant financial burden for

hotel management. Destruction of property is limited to damaged and destroyed items that are due to human interaction and not natural hazards. Financial risks from misuse and abuse of computers include events such as identity theft and data mining. Identity theft can result from issues such as insecure internet networks within the hotel initially affecting the client and eventually causing financial and public relations difficulties.

The operational, strategic and hazard risks were not included in this assessment due to a focus on controllable events that hotel management will be able to prevent within the hotel lobby. These include any and all items that do not involve the use or misuse of hotel lobby computers or the destruction of items within the hotel.

## Assessment

### Risk Assessment Approach

Our methodology will involve researching and collecting data on past and current risk events that have occurred in guest registration areas of the Nittany Lion Inn. Analysts Ryan Glynn and Josh Shtatman will conduct the study. Ryan Glynn is a junior at Penn State University majoring in Security and Risk Analysis in the College of Information Sciences and Technology. Josh Shtatman is a senior at Penn State University majoring in Security and Risk Analysis in the College of Information Sciences and Technology.

We decided to use the Red Team Analysis technique to analyze the data in order to come up with the most plausible situations for the hotel to protect against. This process was performed by thinking of the best ways to exploit an insecure network and unwatched lobby. Items were written down and a list was composed of all possible risks. These risks were then prioritized and ones with next to zero probability were removed.

Our methodology will then be put into action. First we will interview managers and front desk employees and will gather data concerning past risk events in this critical area. We then will collect survey data during the period of September through November, 2010. The data collected will be based on interviews of The Nittany Lion Inn managers and employees concerning potential financial risks associated with the guest registration area. The survey instruments will consist of critical questions concerning access to hotel financial risks in guest registration area that may or may not be secure. We also will detail the current security features of the guest registration area. All of the possible financial risks associated with the guest registration area will then be prioritized and calculated in order to qualitatively explain the most important items secure. These items will be identified using a 3 x 3 risk-level matrix which contains the risk classifications of "low", "medium" and "high".

## System Characterization

The hotel system contains many possible exploits within the lobby but we have identified the guest registration area as the most critical area to focus on for this assessment (see Attachment 2 - Figure 1 which outlines the Nittany Lion lobby and guest registration area). Figure 2 contains a diagram which shows the various levels of priority for each of the inputs and the corresponding processing that would improve or limit the output (Floor Plan 1). The most serious risk in the guest registration area is the lapse in computer security resulting in potential theft of credit card information or other personal data. In addition, some items in this area run a risk of being physically stolen (e.g., cash from a safe), causing direct financial loss to the hotel. There also are items that can cause indirect financial loss through manipulation such as hotel information theft and theft of customer credentials. All of these potential risk factors will be individually analyzed and then prioritized.

The system inputs consist of employees, customers, and visitors. The highest priority input in terms of financial security of the hotel lobby guest registration area is the employee. In addition, other processes the employee must go through to reduce risk includes training sessions on the computer and

safety equipment, along with emergency situation training. Computer skills and training on financial software is the highest priority because of the need for well trained employees who must deal with computer software and financial transactions as well as the customer's personal and financial records. Safety equipment training is of medium priority as it helps reduce the risk of financial loss in the event of a robbery or theft because it would instruct the employee how to operate items such as security cameras and locks. Along with this, employees will need emergency training for instances such as robbery, so that the employee will know exactly what they should to do protect both themselves and the financial assets of the hotel. If the employee successfully goes through all of the processes, the outputs will result in secure computers and safe deposit boxes as well as reduction in the probability of a liability issue.

The customers and visitors both fall under the medium priority in terms of security. Since the wireless network can be accessed anywhere within the Nittany Lion Inn, securing the router and network is the top priority from the customer and visitor inputs (Whiskers 1). While the focus of this analysis in on the guest registration area, both the computers behind the registration desk as well as lobby computers in this area will need to be secure. In order to secure these computers (and others in the hotel), the processes of encryption, connection keys, and lobby surveillance are key aspects to improve the output. Encryption and connection keys will reduce the amount of unauthorized people accessing the wireless network and in turn, reduce the chance of identity and information theft. Lobby surveillance will allow for hotel management to stop or catch any actions that may have caused financial problems to the hotel. All of these processes are of high priority and if all are enacted, the outputs would be a highly secure lobby with a lowered chance of theft or damage to property.

## IV. Threat Statement

After looking into the Nittany Lion Inn's setup for their lobby, we determined that there are three primary threats to the hotel's financial security within the lobby. The sources and the potential financially related damages are shown in the chart below. High priority threats are marked with an "H", medium priority threats are being marked with an "M", and low threats are marked with an "L".

| *Source* | *Potential Threats* |
|---|---|
| *Employee* | ***H:***<br>• *Information Theft/Altering*<br>• *Computer/Network Abuse*<br><br>***M:***<br>• *Physical Theft of Property*<br><br>***L:*** *N/A* |
| *Customer* | ***H:***<br>• *Computer/Network Abuse*<br>• *Information Theft*<br>• *Robbery/Physical Theft*<br><br>***M:***<br>• *Property Damage/Destruction*<br><br>***L:*** *N/A* |
| *Visitor* | ***H:***<br>• *Computer/Network Abuse*<br>• *Information Theft*<br>• *Robbery/Physical Theft*<br><br>***M:***<br>• *Property Damage/Destruction*<br><br>***L:*** *N/A* |

## V. Risk Assessment Method and Results

After identifying the potential sources and threats to the financial security of the Nittany Lion Inn, hotel employees were asked a series of questions concerning the security credentials of the hotel (Attachment 4 Figure 1 lists the survey questions asked of the employees). Employee answers were

analyzed and we then compared their answers to information and research findings concerning threat topics. The chart below outlines the observations and the potential threats related to these observations. Items included in the chart are 1) observation number, 2) the source of possible threat, 3) the possible threat itself, 4) the likelihood rating, 5) the impact rating, and 6) the P.I. Matrix rating. For all ratings, the letters "H", "M" and "L" are substituted for high, medium, and low respectively. An in-depth explanation of the observations and their ratings is explained below the chart.

| # | Source of Threat | Possible Threat<br>"Related Question(s) Asked" | Likelihood Rating | Impact Rating | P.I. Matrix Rating |
|---|---|---|---|---|---|
| 1 | Employee | Information Theft/Leak<br>1) "What are employees able to do on the computers that store client information and hotel information?" | H | H | H |
| 2 | Customer/Visitor | Internet Abuse/Information Theft<br>1) "What form of encryption does the wireless have?"<br>2) "Are there restrictions on the customer's wireless access?"<br>3) "Do you have any employees that watch for suspicious network activity?" | H | H | H |
| 3 | Customer/Visitor | Hotel Information Theft<br>1) "Are the register computers located on the same wireless network as the customer's wireless?" | H | H | H |
| 4 | Customer/Visitor | Property Damage/Theft<br>1) "Are there security cameras?" | M | M | M |
| 5 | Employee | Customer Information Theft<br>1) "How is customer information entered, stored, and kept?" | M | H | H |
| 6 | Employee | Employee Theft<br>1) "How do you currently deter employee theft?" | L | M | M |

All of the observations were based on a questionnaire asked of 3 employees working at the guest registration lobby on October 3rd 2010. To see the full questionnaire, refer to Attachment 4 - Figure 1. The P.I. Matrix rating is based on a 3 by 3 matrix of likelihood and impact, which is presented in Attachment 4 – Figure 2.

The first observation was based on the question "What are employees able to do on the computers that store client information and hotel information?" In response employees stated that they

had the ability to access the internet and any page on it, but only with management approval. However, this is only true if the employee chooses to disclose that they are visiting websites that are not affiliated with the hotel. This policy poses an issue with security because employees have the ability to go to any website, even websites that result in harm to the computer or organization or information theft. The only current mitigation control is the hotel's policy which suggests that they ask for permission beforehand. A potential way to fix this large security hole is to disable access to any website not authorized by the hotel. This change can be done by altering the router settings to block the registration computers from accessing any sites except the ones on a specific list.

The second observation was based on three questions asked to the individuals 1) "What form of encryption does the wireless have?" 2) "Are there restrictions on the customer's wireless access?" 3) "Do you have any employees that watch for suspicious network activity?" The employees responded that the wireless has no encryption at all. This finding poses a huge issue not only for the hotel's security but also for security of customer information. A lack of encryption will allow any person within range to connect to the network and search the network for any interesting information. This problem can easily be fixed by upgrading the encryption to WPA-2 encryption as well as having an authentication key that changes bi-weekly for customers.

The third observation was based on the question "Are the register computers located on the same wireless network as the customer's wireless?" The answer to this question states that both types of computers are located on the same network. This poses a very high risk issue of devious or curious customers trying to see what information they can get about the hotel or its customers. This can cause a very expensive loss in information and possibly liability lawsuits from the affected customers.

The 4$^{th}$ observation was based on the question "Are there security cameras?" In response one employee stated that there are security cameras throughout the hotel. This reduces the likelihood of theft/robbery from a "high" to a "medium" level due to the declination of crime when people feel they

are being watched (Tanneeru 1). This current mitigation of the risk is the best way for the hotel to prevent the crime. Assuming that there is someone monitoring the cameras at all times and as long as the cameras work and record at all times of the day, there are no other suggestions for improvement in this area.

Observation 5 was based on the question "How is customer information entered, stored, and kept?" The answer given by the employees was that customer information was only stored for a set period after they leave, it is then erased. The two main issues here are where that information was stored between when the customer leaves the hotel and when this information is deleted. Because this information is stored on a computer connected to the same network as the customer wireless then there is a very large security issue. The mitigation should be improved so that the information is stored on a computer on a separate or more secure network than the customer network.

The employee given answer to the last question "How do you currently deter employee theft?" was that the hotel will punish employees for taking absolutely anything that doesn't directly belong to them, including items such as hotel pens. The punishment depends upon the level of theft including and up to termination. This policy is by far the best already implemented security policy by the hotel as fear of being caught would be a huge deterrent of employee theft. There is nothing else at this point that is really necessary for them to implement for this mitigation. However, further investigation is required to determine whether employees have options for notifying management of observed theft such as a hotline or other technique.

## VI. Summary

There were a total of 6 primary observations made about possible threats based on a set of 8 questions asked to three employees that worked in the guest registration lobby. Due to the current lack of security implementations and the high impact costs of the majority of possible threats, most of the threats are a high priority. Policies concerning employee theft appear to be appropriate although more

information concerning the manner in which such theft is caught and procedures employees follow to identify another employee engaging in theft would need to be identified. This threat can be improved upon without implementing features that are more costly than they are worth. However, the other security threats are more serious. The network security needs to be encrypted and there needs to be a bi-weekly changing key for customers. In addition, the register computers need to be on their own network so that customers can not attempt to access hotel or client information. For more detailed information on what and how to implement these security fixes, refer to Attachment 3.

## *References*

Enz, Cathy A. “Safety and Security in U.S. Hotels.” The Center for Hospitality Research. Cornell University, n.d. Web. 12 Sept. 2010. <http://www.hotelschool.cornell.edu/research/chr/pubs/reports/abstract-15092.html>

"Floor Plans." *The Nittany Lion Inn*. Penn State, n.d. Web. 24 Sept. 2010. <http://www.pshs.psu.edu/NittanyLionInn/pop_floorplans.htm>.

"Hotel Risk Analysis." *Hotel Risk Analysis*. N.p., n.d. Web. 12 Sept. 2010. <http://hotelriskanalysis.com/>.

Ogle, Josh. "Hotel Network Security: A Study of Computer Networks in U.S. Hotels." *The Center for Hospitality Research*. Cornell University, n.d. Web. 12 Sept. 2010. <http://www.hotelschool.cornell.edu/research/chr/pubs/reports/abstract-14928.html>.

Population, By. "State College, PA Crime Rate Statistics - CLRSearch.com." *Real Estate Search Engine - CLRSearch*. Web. 23 Oct. 2010. <http://www.clrsearch.com/RSS/Demographics/PA/State_College/Crime_Statistics>.

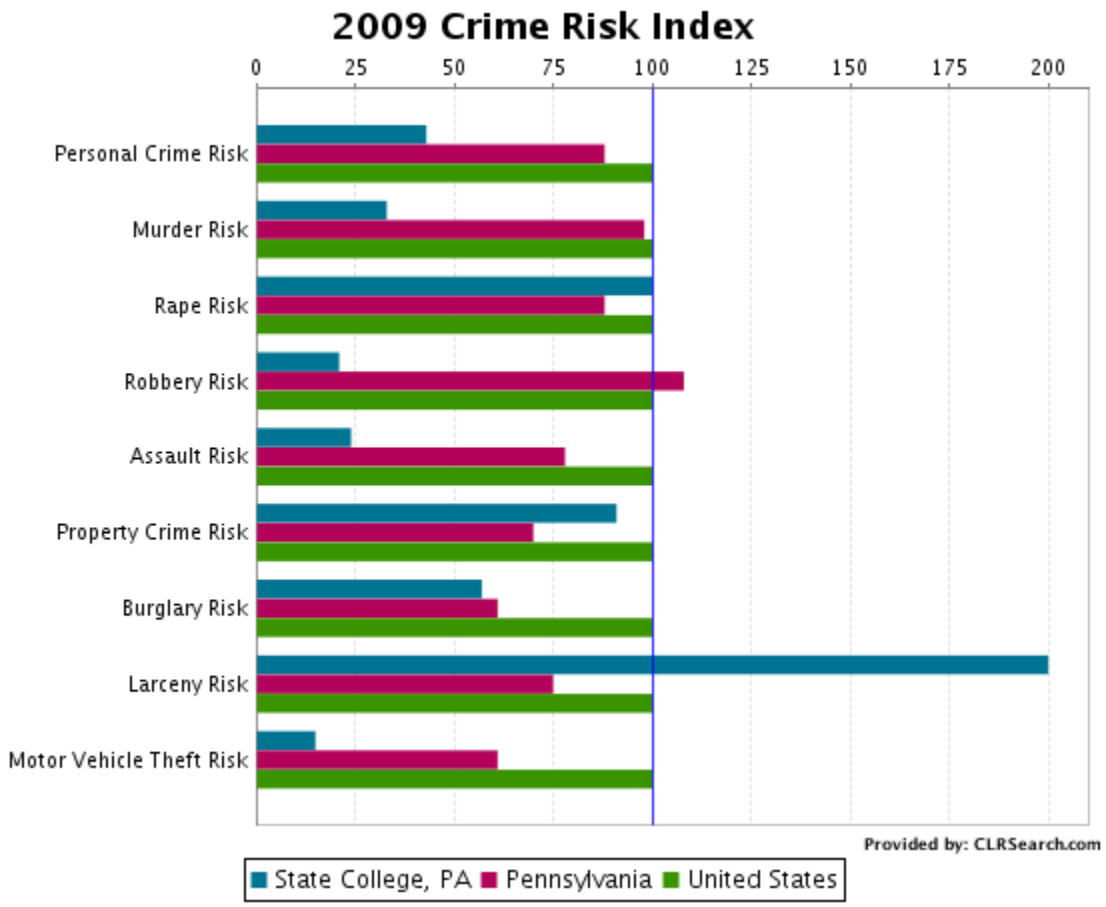
Stephen Rushmore. "MANAGING RISKS PART OF MANAGING HOTELS.” *Lodging Hospitality* 1 Mar. 2010: ABI/INFORM Global, ProQuest. Web. 23 Oct. 2010.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. "Risk Management Guide for Information Technology Systems."*National Institute of Standards and Technology*. N.p., July 2002. Web. 25 Sept. 2010. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.

Tanneeru, Manav. "'Ring of Steel' coming to New York." *International CNN Technology*. CNN, 3 Aug. 2007. Web. 2 Oct. 2010. <http://edition.cnn.com/2007/TECH/08/01/nyc.surveillance/index.html>.

"Whiskers Lounge: The Nittany Lion Inn." *HappyValley.com*. N.p., 2007. Web. 25 Sept. 2010. <http://www.happyvalley.com/posts.php?id=1412>.

*Attachment 1 – Fact Sheet- Crime Stats of State College*




| Crime Statistics | State College, PA | Pennsylvania | United States |
|---|---|---|---|
| Personal Crime Risk | 43 | 88 | 100 |
| Murder Risk | 33 | 98 | 100 |
| Rape Risk | 100 | 88 | 100 |
| Robbery Risk | 21 | 108 | 100 |
| Assault Risk | 24 | 78 | 100 |
| **Property Crime Risk** | **91** | **70** | **100** |
| Burglary Risk | 57 | 61 | 100 |
| **Larceny Risk** | **200** | **75** | **100** |
| Motor Vehicle Theft Risk | 15 | 61 | 100 |
| Total Crime Risk | 63 | 72 | 100 |

The information above gives justification for the reasoning of our focused scope. As shown above, the highest two crimes that relate to businesses are larceny and property crime. These crimes are extraordinarily high so they should be of top priority for the state college area.

## *Attachment 2 – Diagram*

**Figure 1 -** Diagram of the first floor of the Nittany Lion Inn, highlighting the critical area that we are analyzing. This area defines the scope at which our assessment is focused on.

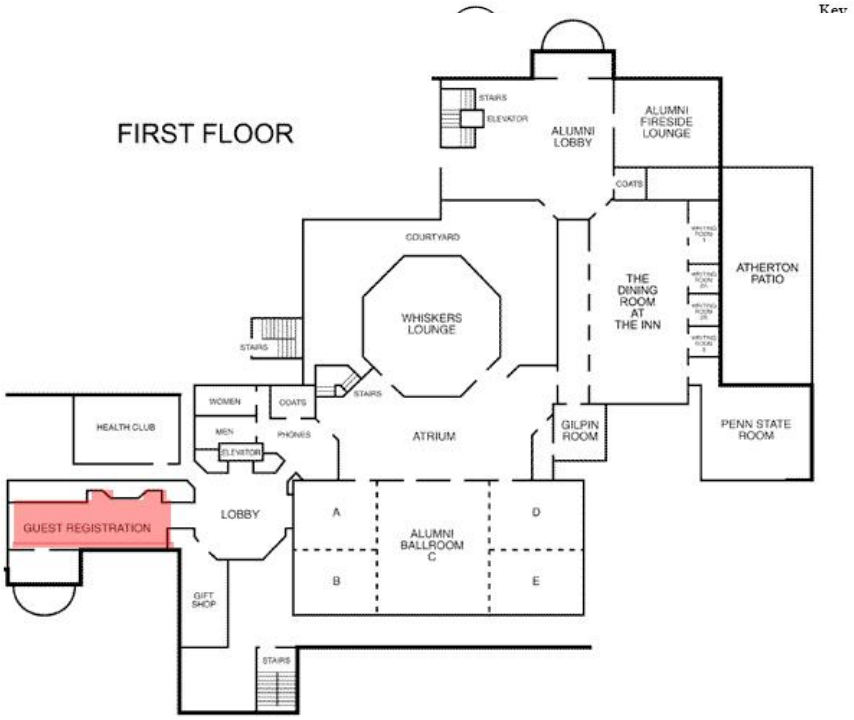
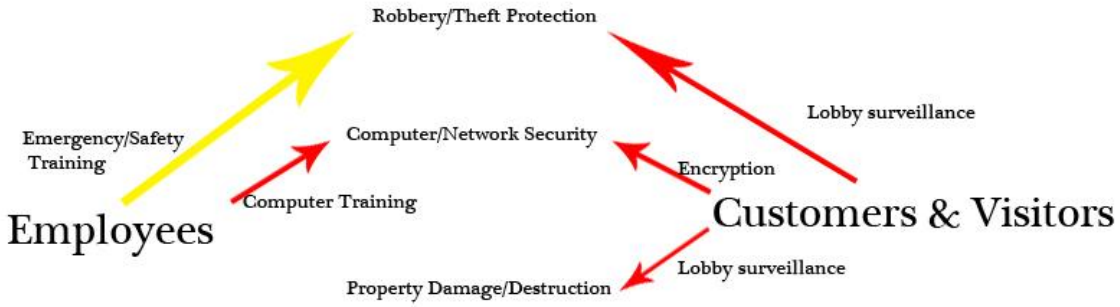



**Figure 2 -** Diagram showing the inputs and outputs and the best processes to obtain the desired output. The large text "Employees" and "Customers & Visitors" shows the 2 inputs from which risk can come from. The colored arrows explain the areas that the inputs can cause damage in. The text next to the arrows states the methodology that can help prevent such an even from occurring. The items that the arrows are pointing to, show the area that the inputs affect. The colors of the arrows represent the priority of such training.




Floor plan image taken and altered from the original at: http://www.pshs.psu.edu/NittanyLionInn/pop_floorplans.htm

## *Attachment 3 – [Appendix C, NIST 800-30 Summary Table]*

| (1) Risk (*Vulnerability*:Threat Pair) | (2) Risk Level | (3) Recommended Controls | (4) Action Priority | (5) Selected Planned Controls | (6) Required Resources | (7) Maintenance Requirement & Comments |
|---|---|---|---|---|---|---|
| *Employees have unrestricted internet access on customer information computers*:Employees are able to steal, or unintentionally leak, hotel or customer information. | **High** | • Disable non-hotel approved website access | **High** | • Disable non-hotel approved website access | • 5 hours to reconfigure router and test the network | • No required change in regular network maintenance |
| *Unsecure wireless network*:Customers & visitors are able to perform illegal activities on hotel wireless. Including but not limited to stealing customer information via packet sniffing and illegal file downloading. | **High** | • Upgrade encryption to WPA-2 encryption<br>• Bi-weekly customer authentication key change | **High** | • Upgrade encryption to WPA-2 encryption<br>• Bi-weekly customer authentication key change | • 2 hours to reconfigure router and test the network<br>• 1 hour twice a week to change authentication key | • 1 hour twice a week to change authentication key |
| *Register computers are on same network as customer wifi*:Customers & visitors are able to steal private hotel information including credit card information and bill information via remote access to the register computers. | **High** | • Attach the register computers to a separate network | **High** | • Attach the register computers to a separate network | • Price of a second router and a maximum of 10 hours to install the new network. | • Regular network maintenance |
| *Possibility of faulty computer cameras:*Customers might be able to damage, destroy or steal hotel property. | **Medium** | **N/A** | **Low** | **N/A** | **None** | • Regular security camera maintenance |
| *Register computers are on same network as customers wifi:*Employees are able to intentionally or unintentionally steal/leak customer billing and personal information. | **High** | • Attach the register computers to a separate network | **High** | • Attach the register computers to a separate network | • Price of a second router and a maximum of 10 hours to install the new network. | • Ensure that the information is only stored as long as it is needed |
| *Faulty security cameras:*Employees might be able to steal hotel property. | **Low** | **N/A** | **Low** | **N/A** | **None** | **None** |

(1) The risks are output from the risk assessment process
(2) The associated risk level is the output from the risk assessment processes
(3) Recommended controls are output from the risk assessment process
(4) Action priority is determined based on the risk levels and available resources
(5) Planned controls selected from the recommended controls for implementation
(6) Resources required for implementing the selected planned controls
(7) Maintenance requirement for the new or enhanced controls after implementation

## *Attachment 4 – Questionnaire and P.I. Matrix*

Due to the sensitive information that could be leaked through the interview questions in Attachment 4 – Figure 1, the employee wished to remain anonymous. The questions asked included the type of access and restrictions the employees had on the computer network. Other questions such as physical security and employee theft were also answered.

These were the right questions to ask because we are focusing on the computer financial risk and property damage. As seen in Attachment 1, Larceny and Property Crime are in the top three highest crime risks in State College. Larceny includes theft of personal information such as a person's SSN, and credit card information.

**Figure 1:**

The questions asked to the employees and their respective answers.

**"What are employees able to do on the computers that store client information and hotel information?"**

Internet access if manager approves, otherwise it is just the hotel registration program.

**"What form of encryption does the wireless have?"**

There isn't any.

**"Are there restrictions on the customer's wireless access?"**

No there aren't.

**"Do you have any employees that watch for suspicious network activity?"**

No we don't.

**"Are the register computers located on the same wireless network as the customer's wireless?"**

Yes they are.

**"Are there security cameras?"**

Yes, all throughout the hotel.

**"How is customer information entered, stored, and kept?"**

It is removed a set amount of days after the customer checks out.

**"How do you currently deter employee theft?"**

Taking of anything, including pens is highly looked down upon.

*Attachment 4 – Questionnaire and P.I. Matrix Continued.*

**Figure 2:**

A 3x3 P.I. Matrix which illustrates how the P.I. Ratings were formed in the assessment above.