UNIVERSITY OF VICTORIA SOFTWARE ENGINEERING

# CASE STUDY : PHYSICAL AND ENVIRONMENTAL SECURITY UPPERTON

Braden Simpson
braden@uvic.ca
V00685500

April 11, 2013

## 1 INTRODUCTION

Upperton, the city of approximately one million people, have upgraded their IT systems and infrastructure to accomodate the higher technogoical needs of their people. The new systems feature decentralized aspects, such as department specific structures, and other centralized services, such as email.

A new Chief Sectunity Officer (CSO) has been hired to create short, and long term plans for the security of the new systems in Upperton. These plans will replace the simple, quick policies setup in the interim. First, the CSO must complete an in-depth investigation on the laptop theft that had happened, and the whole security systems. Then the plans must be put in place to prevent

## 2 INITIAL INVESTIGATION

The initial investigation should be conducted immediately, evaluating exactly what went wrong when the laptop had been stolen the night prior. This will provide what the baseline is for the organization which can then be used in the Gap anaylsis[1].

[1] Gap analysis is a method used to compare actual performance with planned performance. http://en.wikipedia.org/wiki/Gap_analysis

The investigation should go as follows:

**Root Cause** The first part of the investigation should find out exactly what happened, and determine all the contributing factors to the laptops theft. (i.e. was the door left unlocked? did the employees at the building not have the proper security training? did they not understand the value of the information on the laptops? etc.)

**Potential Mitigating Factors** Next, the investigation needs to define possible methods for mitigating the problems outlined above. These should include other potential ways to mitigate related incidents as well.

**Recommendations** Short, mid, and long term recommendations, based on the cost-gain ratio of the mitigating factors. The quick, easy methods to prevent the problems should be done first, in addition to the critical problem fixes, such as ensuring the staff locks the doors every night.

**Present Recommendations** In order for the situation to be taken as seriously as it is, the problem must be presented to the people with control of funds, and power to take action on the recommendations. This means that the plans need executitve buy-in, which gives the CSO enough funding to implement the procedures needed.

# 3 Short Term

There are many solutions which can be added in the short term, which I will address in this section. The main solutions are as follows:

**Stricter Access Rules** This is a very important and good general practice for organizations to implement. The general idea is to create a need-to-access rather than a want-to-access model for access to sections of the data centres. Stripping access away from every person that isn't specifically required to be in the data centres, regardless of ranking in the comapny, etc.

**Education on Current Infrastructure** This is something that must be done immediately, as the entire policies that govern the security rely on everyone following them or the system crumbles. This would require that people have education sessions if needed, there would be posters, and informative sessions, as well as security quizzes taken periodically.

**Monitoring and Surveillance** Another short-term solution would be to install a system to monitor the entry of certain areas, or improve the alarm systems that are in place, a simple CCTV system or motion alarm system would be an easy way to monitor entrance to certain areas.

**GAP Analysis (Baseline)** Construct the baseline for the GAP analysis to be compared against in the long-term. This is a common tool used to evaluate a plan's performance.

# 4 LONG TERM

In this section, the long-term solutions are discussed. These would be harder to accomplish, long standing goals for the security plan.

**Complex Keycard Access System** This is a method employed by many large companies with that have important access policies and restrictions (i.e. access to the data centres). The system would have keycards for each employees with specific access rights defined in them, and there would be readers at each door. The more important rooms could even have the *Mantrap*[2] 2 part access system.

**GAP Analysis (Evaluation)** Evaluating against the baseline created in Section 3 will provide a good means to show the company's acceptance of the new security plan and how well it is performing.

**Better Physical Security** This means rebuilding or reinforcing parts of the data centres that might be more prone to attack. For example, the access to the most critical data storage areas might have thicker concrete around them, or securing the doors with anti-pry plates around the handles.

**Hiring Security Personnel** If the security measures requires 24/7 surveillance, another means of creating more security is to hire people to physically watch the centres, whether through CCTV or onsite surveillance.

# 5 FUNDING

One of the most important steps of the security plan is to obtain the funding required to imeplement the whole plan, including short and long term goals. The funding can be a very difficult aspect. However, the recent laptop theft can be leveraged to show the importance of a good security plan for their data centres.

The CSO should plan a meeting with the CFO, or other top level executives to present the investigation on the laptop theft, which will gather awareness and a sense of necessity for the new plan.

Some of the solutions mentioned in this report have large monetary or time consuming costs, such as the keycards, hiring more personnel, etc. If the CSO cannot get all the required funding then the most important solutions must be found. This would be done by doing a gain-cost analysis on the solutions in place.

[2] Mantrap system for access has 2 doors which open and close and keep the accessor in the area between the two, and requires the first to be closed for the second to open