University of Victoria, Software Engineering

# Case Study 11: Physical and Environmental Security

Jordan Ell
V00660306

April 7, 2013

## 1 Introduction

This case study is focused on the physical and environmental security of the Upperton city IT governance structure. The scenario states that a new Corporate Security Officer has been added to the security team while a laptop was recently stolen from the data center in the previous week. The CSO has been tasked with the job of imporiving information security practises for the city's data center. This includes short and long term goals as well as obtaining funding from the city to implement these goals. These rest of this case study will be laid out as follows. First, I will explain what should be immediatly done about the stolen laptop with an investiagion. Next, I will explain both short and long terms plans to improve the physical and environmental security. Lastly, I will explain how possible funding could be achieved to help implement the aformentioned goals.

## 2 Investigation

Due to the laptop theft, an immediate investigation should take place involvind the circumstances and damage caused by the theft. The investigation should focus on the significance of the theft. How easily were the theives able to obtain the stolen laptop? Did they have to go through already implemented security measures, or are there back-doors in place in which a thief might circumvent the whole security infrastrucutre in order to steal the laptop. This emphasis on significance should outline exactly where the weak spots are in the pre existing security environment and should be the main focus of adaptation of a new security plan. The significance of the theft report should also focus on what was actually stolen. Are laptops just laying around the data center unattended? How easy is it for a theif to steal a rack server. What information is being placed on these machines that may be physically less demanding to steal. If unencrypted data is being stored on a non secured laptop in the data center, this is a serious cause for concern.

## 3 Short Term Goals

The easiest short term goal, is to ensure that everyone is following pre existing security architecture. This will at the very least help with liability through accounting for legitimate actions in the data center warehouse. The second quick solution to laptop thefts are to reduce the potential points of entry to only secure entry points. If the data center has a key card door, but at the same time has a ground level window or a back door (even if locked) this is a large concern. The data center should be reduced to the single secure entry point where actions are accounted for (employees entering and leaving the data center).

A second (possible) short term goal would be to install CCTVs in the data center. CCTVs are relatively inexpensive and can be installed with general ease. This is what makes them a good potential short term security measure as they can be up and running relatively quickly. A few things to note about the CCTVs in the data center. First, they should only be installed where they cannot be tampered with or otherwise turned off without the camera itself, or other cameras catching the action in their field of view. This will stop theives from simply disabling the cameras on their own. Second, the footage captured from the CCTVs should be stored externally from the data center they are monitoring. Theives should not be able to break into both the recorded data center as well as the footage collection facility. This will stop theives from simply stealing the recording of the break in.

A final short term solution of the breakin is to ensure that only those employees with a need-to-access authority actually have access to the data center. Having too many employees with hightened privaliges is a bad idea for security as the accountability decreases as volume increases. Limiting the data center to a need-to-access authority will impede potentially hazardous employees who normally would have no need to enter the data center other that to steal from it from entering. For most non secure data centers this can be achieved with simple key privaliges.

## 4 Long Term Goals

The first long term goal I would suggest that the CSO implement, is key card access with proper authentication procedures in place. Having key card access improves liability among employees as logs of entering and exiting the data warehouse can be kept. These logs allow for future analysis in case of any mishap in the data center. You can check to see who was in the room at the time. The key card access can also help raise suspicious activity to the IT team. If one employee is rapidly entering and exiting the data center, this may be cause for concern, or if an employee enters and does not exit for a long period of time, this may also be a concern. The second side of key cards is to have proper procedures in place to allow for need-to-access authority to be given to the correct people. Key cards can be set up to only allow certain employees into specific rooms of a building. Have a proper, documented, procedure in place for these elevated privaliges will also allow for higher security standards as it will be known who has access to which equipment.

A second long term goal will to be to analyse the types of threats the compeny has to deal with on a regular or potential basis. If the office resides on the ground floor of a building, windows may cause a very large risk to potential physical envrionment harm. A plan to potentiall bar, or install shatter resistant windows may be a good step in the right direction to securing a large building in the log term.

## 5 Funding

In order to implement some of these suggested short and long term security measures, proper funding must be in place, especially for more costly measure such as CCTVs, key cards, and window installation. The best way to achieve funding for security projects, as with every case study done in this class so far, is to obtain corporate level buy-in and explain the situation from a business goal stand point. If the executives of the company (or city of Upperton) can view physical security as a business expense, they may be more willing to hand over more money for potential security measures.

To explain physical security as a business expense, I would recommend that the CSO explains the cost of a data breach or physical break in to the corporate level executives. This involves explain physical costs as well as potential damages from following lawsuits caused by the loss of private data from citizens. The physical costs would be that of the loss of equipment. Examples of this might be the laptop theft (the cost of the laptop), damages to locks from the break in, and damage to heavy equipment during the break in (this could be damaged rack servers, or heavy and expensive main frames). The larger for potential loss is the damage from stolen information. If credit card information is stolen, lawsuits could become an imminant threat to Upperton. These monotary losses could far exceed physical damage costs and should be mitigated through proper physical environment security measures.

With these explination, any CSO should be able to find funding for the security measures that I have outlined in the short and long term goals previously. The funding supplied should also account for future upgrades, future damages, and employee salaires to have a security team that can monitor and act on security infrastructure.