Information Security Exercise

Hans Georg Schaathun
Høgskolen i Ålesund

Week 8 Autumn 2011

Task Perform a risk assessment for a dentist's surgery as described below using a risk management framework of your choice.

Objective Your goal is to become familiar with a structured and systematic approach to risk analysis, and be able to use it effectively.

Submission
1. The submission should be in the form of a single PDF document.
2. Name and email address must display clearly on the first page.
3. *Deadline* Monday 17 October 2011 by 6am in Fronter.

Remember
1. Make reasonable assumptions for any details not mentioned in the assigment.
2. State all assumptions explicitely.
3. Check the threats identified against lists of threats in the textbook and/or other sources.
4. Cite the documents you use.

1 The surgery

A floor plan is shown in the figure. The surgery has twelve staff, including five dentists, five assistants and two receptionists. The latter are responsible for the reception and the switchboard, arranging appointments, setting up invoices and receiving payments.

1.1 IT solution

All the dentists have their own PC with digital X-ray, and additionally, there are two office-PC-s in the reception. All the PC-s are connected on a LAN which also includes shared printers.
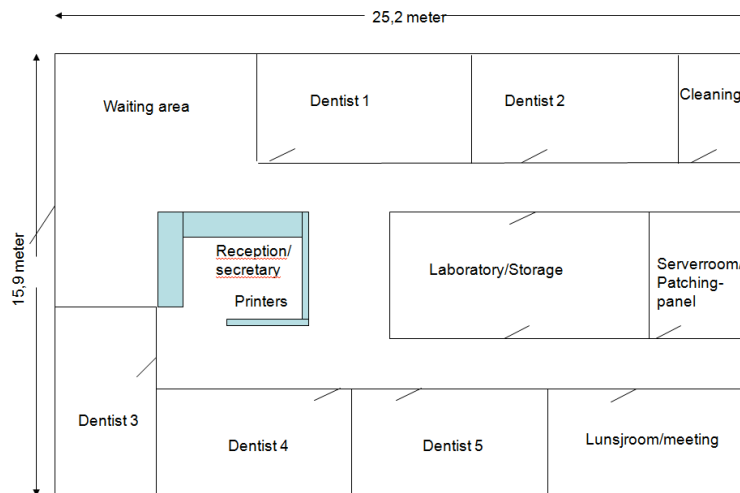
Figure 1: Floor plan for the surgery.

1.2 Dentistry Computing System

The surgery is connected to a data centre with an IT provider, running all applications on servers in the data centre. The PC-s run thin clients.

The main system, used by everyone in the surgery, is a spesialist system for denists' surgeries. It has the following modules:

- Patient administration, with all the appointments
- Patient records, with dental data for all patients
- Digital x-ray, taking x-ray pictures, storing them in the patient records, and viewing

1.3 Communication

The surgery is connected to the IT provider via a rented line from Telenor. Onwards Internet connection is via a FireWall with the provider.

It is the IT provider who has the contract with Telenor. The surgery has a total plan with the IT provider, including the communication line. The agreement is 99.98% uptime between 8.00 and 18.00 on week days.

1.4 Office Support

In addition to the specialist system, all the PC-s also have access to MS Office applications. This is also run on the IT provider server. Word and Excel are used only a

little, but everyone uses Outlook for email. Appointments in the specialist system are not integrated with the Outlook calendar. Incoming email is scanned and filtered for virus and spam.

1.5 Internet

All staff has Internet acces on the thin clients and access to remote application in the data centre. Firewall, virus protection and antispam are implemented in shared solutions with the IT provider.

1.6 Web pages

The surgery has a standardised solution for web presentations, developed by the same supplier as the spesialist system for dental surgeries. The contents is adapted by one of the dentists with a special interest in IT. He is self-learnt. The pages allow clients to make and change appointments.

1.7 Payment

A payment terminal is installed in the reception. Communications with BBS uses the same line to the IT provider, and on a dedicated line from the provider to BBS.

1.8 Fire and burglary

The surgery has burglary and fire alarms connected to a security company. One of the assistants do not work full time during office hours, but do cleaning as well as sterilising tools and equipment after the office is closed for the day.

Good luck