Risk Presentation

Group 4

Risk #1 – Your access control system uses outdated technology

The technology used in the current card system has been insecure for 18 years

Thieves can clone staff access cards with ease

Guests will lose trust in hotels that can't keep their doors locked

Effective replacements have been available for 14 years

Treatment for Risk #1

Fortunately, replacements are plentiful to come by

The MiFare Plus system is a direct upgrade to the current MiFare Classic system

The current door locks won't even have to be replaced

If Salto your current provider won't upgrade, others will

Risk #2 – The passwords for the database are chosen by staff

The database contains booking information

This database is accessed with a staff ID and a password

This password is chosen by staff members

This makes the risk very likely and the impact high

Treatment for Risk #2

The treatments for this risk are cheap, easy and effective

Having a password policy guides staff members to choosing good passwords

The National Cyber Security Centre recommends choosing three words

You could also implement two factor authentication

Risk #3 - Physical accessibility to networks for guests and conference room/ network segmentation

Guest rooms and the conference centre both contain points able to connect personal devices

Guest rooms contain ethernet ports which allow access to the guest network

Conference centre allows devices to be plugged in for conference reasons

Both could become compromised due to either intentional or unintentional uploading of malware

Treatment for Risk #3

Disallowing any form of uploading onto the guest network from ethernet ports

Devices intended to be used in conference room could be checked by staff beforehand

Anti-virus software or malware detection software on both connection points e.g. network malware boxes for ethernet

Nuclear option – remove all ethernet ports from guest rooms

Risk #4 – The network is encrypted with WPA

The Wi-Fi is encrypted with WPA, a depricated encryption method

WPA is susceptible to Key Reinstallation Attacks

Out-of-date operating systems allow for this vulnerability

Threat actors can intercept and modify packets, making the impact of the risk high

Treatment for Risk #4

Updating all the hotel's machines to the latest version of their respective operating systems

Updating the wireless access points' firmware with a vendor patch – some access points may not receive updates anymore

Purchasing new wireless access points that are WPA3 compliant

Setting the wireless access points to WPA2 and disabling the "EAPOL-Key" option, however this will cause poor connectivity