Physical Security

Introduction to IT Security

Otago Polytechnic
Dunedin, New Zealand

Physical Security

Physical security is

- the most overlooked part of IT security, and
- the source of some of the most easily exploitable vulnerabilities.

It is also a good example of how security is always a trade-off versus convenience.

Servers/Core Hardware

- Should be in locked equipment rooms
- Access should be monitored
- Equipment should be properly secured in racks

Network access

- Unsecured open wired access points should be disconnected.
- Wireless access areas should be mapped out. Avoid giving wireless coverage in areas that are physically insecure.

Work stations

- Should be in physically secure areas.
- May also need to be locked to their locations.
- Should have BIOS passwords (and correct boot device order).
- In some cases, a case lock should be used.
- In some (more extreme) cases, usb and other ports should be disabled.
- Consider hard drive encryption.

Printers

Some printers/copiers/scanners store copies of recent files in memory and need to be secured.

Removable media

- Backup tapes
- USB keys
- Old printouts

May all have sensitive data on them and need to be handled properly

Portable devices

- Portable devices have all of the problems that workstations have, but
- We don't have some of the options of physically securing them.
- Things like hard drive encryption and remote control tools are even more important.

Device disposal

- Anything that stores data should be wiped clean or otherwise disabled before they are taken out of inventory.