**D1 - Review a Recent Development in Technical Support**

A new technology that is becoming increasingly common in (and relevant to) IT technical support is Cloud Computing.  
Cloud computing is the concept of moving all of the processing hardware onto remote servers that are accessed via simpler machines over the internet - ‘The Cloud’.  
Because the hardware & software used to access the cloud services are very simple (usually just a low-end PC and a web browser), on-site maintenance is massively reduced.  
Additionally, all concerns about maintaining data goes to the server hosts. This will be specified in the Terms of Service or another contract.  
Because one cloud hosting service will serve multiple clients, only a single maintenance team is needed for dozens of different client organizations.  
Servers, and the sites they are housed in, cost a lot of money in land, electricity, hardware and cooling systems, that no small organization could afford. However, because many clients are all paying for the service, it becomes possible.  
Cloud-based services are accessed over the internet, meaning that users can work from anywhere with an internet connection - work, home, the commute - which increases flexibility and availability.

A concern with cloud computing is security - all data is being entrusted to a third party. Generally, cloud hosting providers will have privacy policies, security policies or contracts specifying how they will keep data secure, and protected from accidental damage (hardware failure, user error, etc).  
Another issue is that communication between the user and the cloud can be intercepted or hijacked. To protect against this, most companies require users to use a VPN or other software to access the service.  
Because cloud services are accessed remotely, they expose an attack vector not present in a traditional LAN IT system - open communication. Any point on the route between the user and the server becomes an additional vulnerability, as well as the end points of the user’s computer (which may be personal) and the server (which could be attacked directly).