2.5 Disadvantages of virtualization:

1. **Performance degradation:**
   - Performance is definitely one of the major concerns in using virtualization technology. Since virtualization interposes an abstraction layer between the guest and the host, the guest can experience increased latencies.
   - For instance, in the case of hardware virtualization, where the intermediate emulates a bare machine on top of which an entire system can be installed, the causes of performance degradation can be traced back to the overhead d introduced by the following activities: • Maintaining the status of virtual processors • Support of privileged instructions (trap and simulate privileged instructions) • Support of paging within VM • Console functions.
2. **Inefficiency and degraded user experience:**
   - Virtualization can sometimes lead to an inefficient use of the host. In particular, some of the specific features of the host cannot be exposed by the abstraction layer and then become inaccessible.
   - In the case of hardware virtualization, this could happen for device drivers: The virtual machine can sometimes simply provide a default graphic card that maps only a subset of the features available in the host.
   - In the case of programming-level virtual machines, some of the features of the underlying operating systems may become inaccessible unless specific libraries are used.
   - For example, in the first version of Java the support for graphic programming was very limited and the look and feel of applications was very poor compared to native applications. These issues have been resolved by providing a new framework called Swing for designing the user interface, and further improvements have been done by integrating support for the OpenGL libraries in the software development kit.
3. **Security holes and new threats:**
   - Virtualization opens the door to a new and unexpected form of phishing.The capability of emulating a host in a completely transparent manner led the way to malicious programs that are designed to extract sensitive information from the guest.
   - In the case of hardware virtualization, malicious programs can preload themselves before the operating system and act as a thin virtual machine manager toward it.
   - The operating system is then controlled and can be manipulated to extract sensitive information of interest to third parties.
   - Examples of these kinds of malware are BluePill and SubVirt. BluePill, malware targeting the AMD processor family, moves the execution of the installed OS within a virtual machine.

4. **High Cost Implementation**
   - When considering virtualization, the average individual or corporation will incur relatively low costs.
   - However, the implementation expenses for virtualized environment providers can be fairly significant. At some point, hardware and software are necessary, which means devices must be designed, made, or purchased for implementation.

5. **External attacks:**
   - Virtual machines can potentially be infected with viruses, spyware, and ransomware. These attacks can be launched by infected VM images or by people who have not received adequate security training.
   - If attackers gain access to your host-level or VMware vCenter server, this opens doors for them to access other important VMs, or even create a user account with admin rights that could be used over a long period of time to collect or destroy sensitive company data.
6. **Software Licensing:**
   - This is becoming less of a problem as more software vendors adapt to the increased adoption of virtualization. However, it is important to check with your vendors to understand how they view software use in a virtualized environment.