Mobile computing has its fair share of security concerns as any other technology. Due to its nomadic nature, it's not easy to monitor the proper usage. Users might have different intentions on how to utilize this privilege. Improper and unethical practices such as hacking, industrial espionage, pirating, online fraud and malicious destruction are some but few of the problems experienced by mobile computing.



Another big problem plaguing mobile computing is credential verification. As other users share username and passwords, it poses as a major threat to security. This being a very sensitive issue, most companies are very reluctant to implement mobile computing to the dangers of misrepresentation.

The problem of identity theft is very difficult to contain or eradicate. Issues with unauthorized access to data and information by hackers, is also an enormous problem. Outsiders gain access to steal vital data from companies, which is a major hindrance in rolling out mobile computing services.

No company wants to lay open their secrets to hackers and other intruders, who will in turn sell the valuable information to their competitors. It's also important to take the necessary precautions to minimize these threats from taking place. Some of those measures include −

- Hiring qualified personnel.
- Installing security hardware and software
- Educating the users on proper mobile computing ethics
- Auditing and developing sound, effective policies to govern mobile computing
- Enforcing proper access rights and permissions
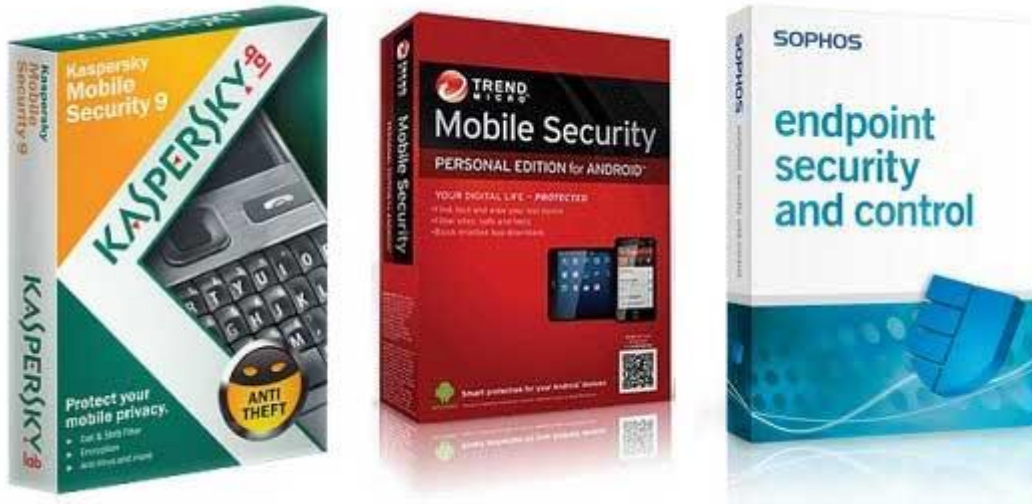
These are just but a few ways to help deter possible threats to any company planning to offer mobile computing. Since information is vital, all possible measures should be evaluated and implemented for safeguard purposes.

In the absence of such measures, it's possible for exploits and other unknown threats to infiltrate and cause irrefutable harm. These may be in terms of reputation or financial penalties. In such cases, it's very easy to be misused in different unethical practices.

If these factors aren't properly worked on, it might be an avenue for constant threat. Various threats still exist in implementing this kind of technology.