SQL Injection is a major issue because it allows someone to gain access or make changes to a system they would otherwise be unable to access or change. It is a major issue because there are many databases that have to be set as semi-accessible to the public, like those accessed by a user login system. SQL injection attempted on a database for this system that has not been protected from these types of cyber attacks will very quickly be breached due to the simplicity of the attacks. The massive amount of data that is now stored, shared, and accessed due to the invention of the internet is another reason this type of attack has become such a major concern since its creation.

The party responsible if data is breached due to SQL injection is two-fold. Both the person committing the SQL injection AND the company maintaining the data are at fault. The person committing the attack should always be considering one of the responsible parties, but in this case, SQL injection attacks have been a common occurrence for such a length of time, and are so easily mitigated, that a company should consider this type of security a minimum requirement for any database before a system becomes a live, functioning program.