Need for transition from modern cryptographic techniques to post-quantum cryptographic techniques

1. Shor's algorithm:

Potential of quantum computers to solve problems efficiently that underpins the widely used cryptography techniques which would break RSA and ECC proving them insecure.

2. Proliferation of quantum technology

Rapid advancement of quantum computers suggests that with significant investments from both private and governmental bodies, post-quantum era is closer rather than further.

3. National security concerns

Data from government and military that holds sensitive information regarding the country cannot be left vulnerable to quantum threats and should be prioritized first.

4. Security and confidentiality

Transition is necessary to mitigate risks from store now depict later threats. To meet regulatory standards for protection of sensitive information, transition is necessary.

5. Future proofing

Adoption of cryptography techniques now will render the future security measures to be impenetrable to threats from quantum computers.

6. Lack of preparedness of current systems

Transition plans are not quite adequate up until now and there is a chance that organizations left behind may have limited time frame to transition that may result in financial stress.

7. Standards development for the community

Engaging in such developments as NIST i.e. National Institute of Standards and Technology will ensure that organizations adopt most secure and vetted options.