Risk assessment for modern day cryptography from quantum computers:

Overview:

Current cryptographic techniques are vulnerable as advancement of quantum computing poses new threats significantly to those that rely upon the use of traditional algorithms. This may include business organizations, private collectors, government bodies or any other imaginable industry that uses modern cryptography. This risk assessment examines such risks associated with quantum computing.

Risk identification:

- Inadequate preparation:
  Lack of transition plans from organizations and failure to implement quantum resisting algorithms risks future vulnerabilities.

- Vulnerabilities in current cryptographic algorithms:
  Quantum computers and its algorithms such as Shor's algorithm can factor large numbers efficiently, breaking algorithms such as RSA and ECC.

- Impact on Data security:
  Data breaches now can be decrypted later which is a serious threat, "store now decrypt later".

- Proliferation of quantum computing:
  As quantum technology advances, access to quantum computers results in increase of threat actors.

Risk analysis

Likelihood of quantum threats:

- Short term: low, quantum computers are yet to advance to a point where current cryptographic techniques are at immediate threat.
- Medium term: Moderate, practical quantum attacks are researched to be possible as the quantum technology advances.
- Long term: High, 10+ years after, numerous threat actors and knowledge of quantum computers is likely to pose new risks.

Potential impact:

- Financial costs due to data breaches, regulatory fines and replacement of security systems.

- Loss of data also results to reputation damage.
- Confidential data loss has severe implications for risks.

Risk mitigation strategy

1. Transition to post-quantum cryptography:
   Adoption of quantum safe cryptographic techniques, regulations and standards.

2. Security audits:
   Evaluation and updating the security protocols and replacing them to meet new standards.

3. Training and awareness:
   Stakeholders must be informed of the risks associated and adequate training must be provided to the staff at hand.

4. Adopting encryption practices:
   Quantum safe algorithms such as lattice-based, hash-based and polynomial cryptography must be integrated.

5. Informed about the technological advancement:
   It is essential to monitor breakthroughs in quantum technology to adapt to the strategies as needed.

Conclusion

Proactive measures are needed to mitigate risks from quantum threats although it does not pose any immediate threats to modern cryptography techniques. Government bodies and business organizations that collect confidential data cannot take risk of a data breach and therefore transitioning to post-quantum cryptographic techniques is a must.

Risk assessment table:

Risks identified	who is harmed and how?	What are you doing to control risks?	What further action can be taken	Who carries out the action?	When is the action needed to be carried out?	Process
1. Inadequate preparation	Stakeholders, business, organization, government	Security audits	Transitioning to post-quantum cryptography techniques	organization	Medium term plan	Doing
2. Vulnerabilites in current cryptography techniques.	Government, business	Informed about technical advancement	Training and awareness	Government, educational bodies, organization	immediate	Doing
3. Impact on data security	Business Government stakeholders	Adopt quantum safe cryptography techniques	Inform and train for awareness	Educational bodies, Business organization	Medium term	To do
4. Proliferation of quantum technology	stakeholders	Inform about technological advancement	Transition and train to adapt to post-quantum computers	Organization, Educational bodies, regulatory bodies, government	Long term	To do