

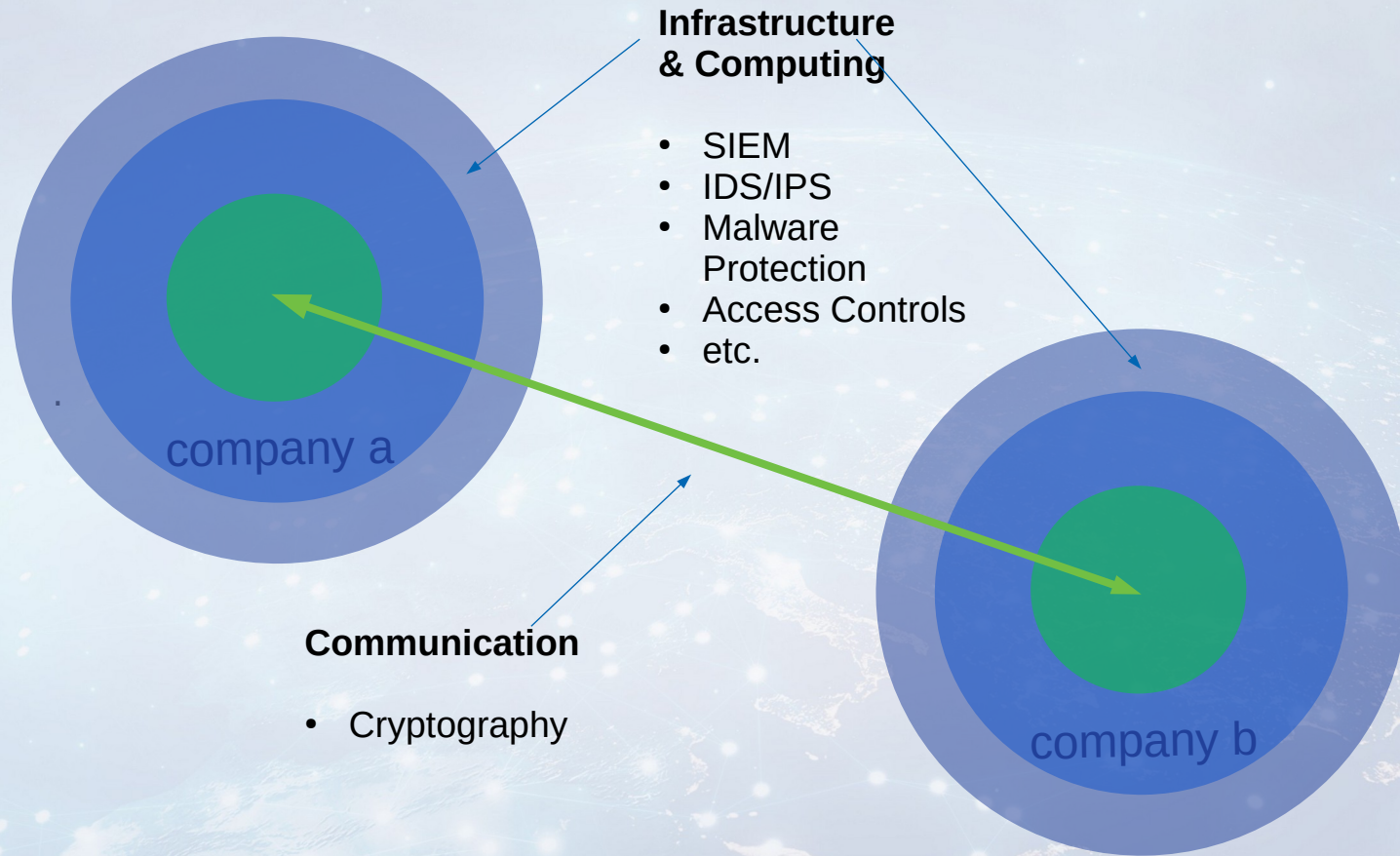
 QUANT-X SECURITY & CODING



Data Protection on Highly Volatile Threat Landscapes

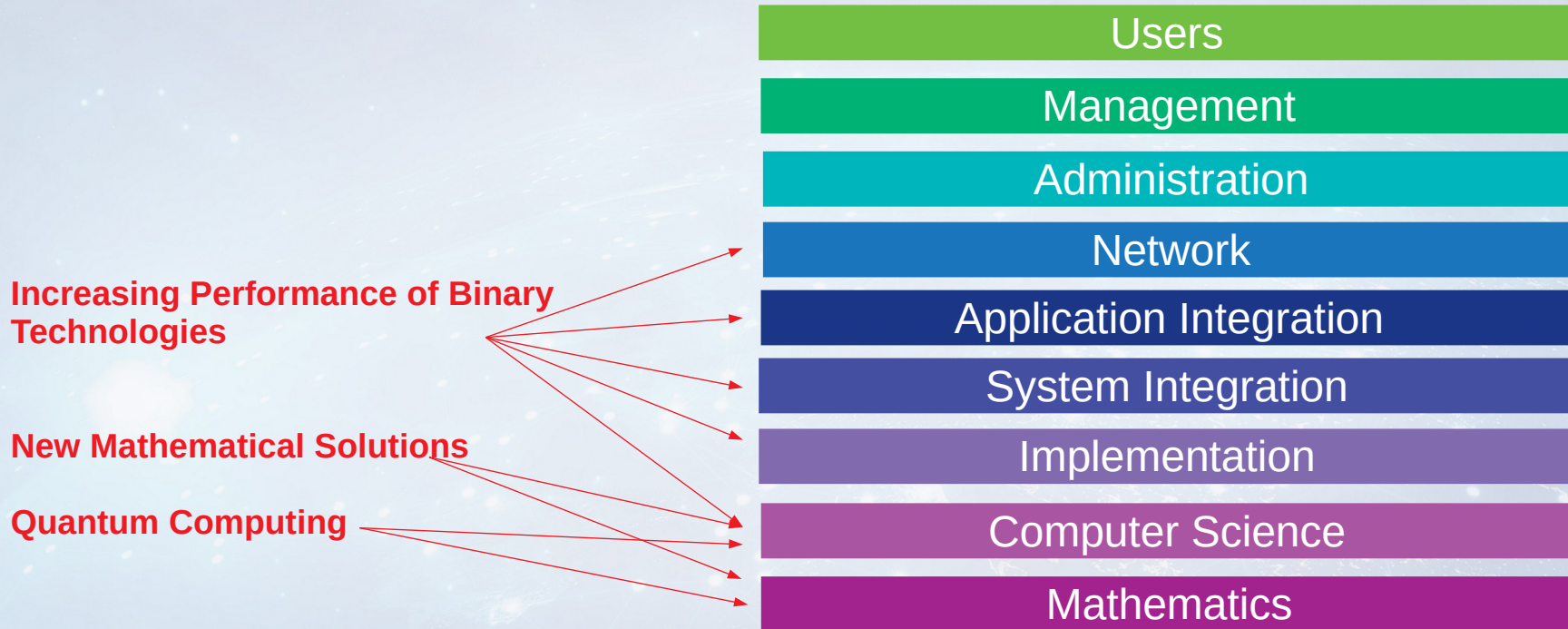
<https://quant-x-sec.com/> | [xb@quant-x-sec.com](mailto:xb@quant-x-sec.com)

# The Unique Meaning of Cryptography in Information Security



# Preserving Privacy in the Face of High Performance Attack Vectors

## THREATS



# Overview on High Performance Attack Vectors - Current

## Threats

- Password and Cryptography Cracking Tools (Hashcat and similar tools)
- Aggregated computing resources and parallelization of attack processes
- New mathematical solutions affecting parameters and configuration of classical crypto

## Countermeasures

Regularly check RFCs and recommendations of official Data Protection and InfoSec institutes for

- 1) Choice of algorithms
- 2) Key length
- 3) Algorithm parameter configuration

... and update your systems accordingly in alignment with depending parties.



# Overview on High Performance Attack Vectors – Near Future

## Threats

Evolving Quantum Computing Technologies will make it possible to decrypt data encrypted by

- 1) Diffie-Hellmann
- 2) RSA
- 3) Elliptic Curves

Timeline: IBM guesses by 2023

## Countermeasures

- 1) Use new post-quantum crypto algorithms for binary technologies  
(NIST standardization round 3: <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions>)
- 2) Homomorphic Encryption (not based on 1) -3) in Threats :-)
- 3) Quantum Communication (new quantum hardware, expensive)



# Identify Assets of High Privacy Criticality by Information Risk Assessment

**Your Business Processes and the respective IT-systems are your Assets!**

**1) Perform a CIA-Rating** on your systems. This will indicate the protection need of the systems. The best candidates for a near time transition to homomorphic encryption are the ones with

- High Confidentiality and Integrity Classification
- Low Availability Rating

The best candidates for post-quantum cryptography are the ones which process data which needs to remain confidential for many years in the future.

**2) Perform an Information Risk Assessment** to consider threats vs. the systems protection need. This will help you to determine which new cryptography you might want to apply to which system.

(Guide for conduction IRAs: <https://www.nist.gov/publications/guide-conducting-risk-assessments>)



# Conclusion

**Stay aware about upcoming threats and solutions.**

**...and**

**Introduce swift crypto patch processes!**

Thank you!!!

Find these slides on <https://quant-x-sec.com/published.htm>

(in the section Talks/Presentations at Conferences and Events)

