Data & Cyber:
Synergy by Design Mindset

Natalia Bakhtina, MBA

For CDAO APEX West

Phoenix, Arizona

December 05, 2023

Agenda

- Data Security: Global Trends

- Protecting Brand

- Data & Cyber: Win-Win

- Strategic Competitive Advantage

- Quantum Computing: Y2Q & Trends

- Quantum: Risk & Opportunities

- Possible Use Cases

- Key Considerations

- Crypto Agility: Data is Key

- Data Awareness: Quantum-Proof Foundation

- Key Takeaways

Global Trends: Growing Importance of Data Security

US$ 9.5 M
the **average cost** of a data breach.
52% of data breaches are caused by
malicious attack

17 %
of all sensitive files are accessible to
all employees. On average, every
employee has access to **15 million files**

22 %
of breaches are dues to **phishing**.
17% - **malware**. 45% - **hacking**.

320 %
rise globally since 2019 in requests for
additional ransom demands

1 in 36
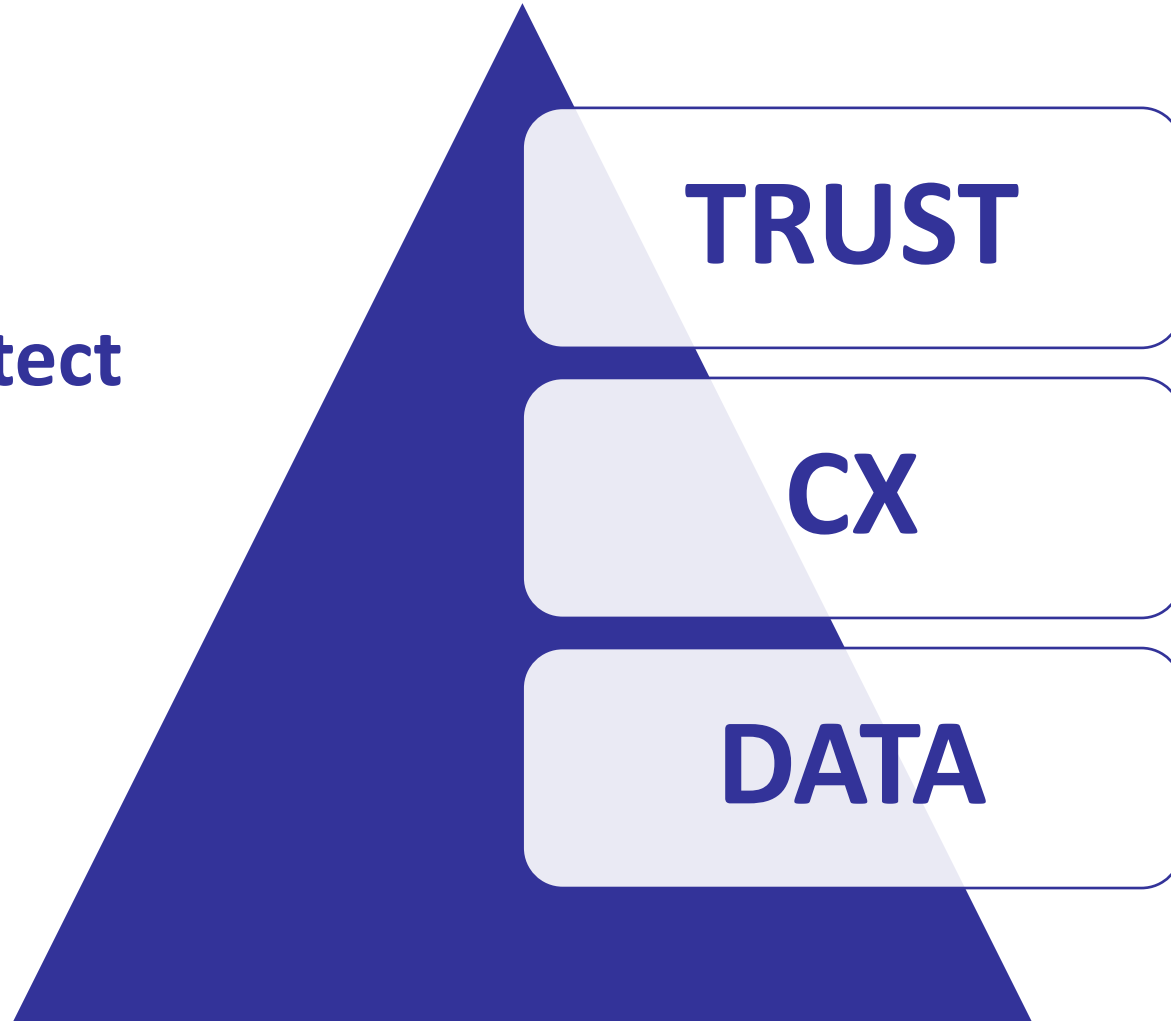mobile devices on average have
high-risk apps

50
days is the average cost in time for a
malware attack. **207 days** - average time
to identify a breach. **280 days** - average
breach lifecycle from identification to
containment.

Data Security: Protecting Brand

TRUST
is the core
we aim to protect

TRUST

CX

DATA

Data & Cyber: Win-Win Partnership

DATA INVENTORY

DATA FLOW

DATA ARCHITECTURE

DATA RESIDENCY

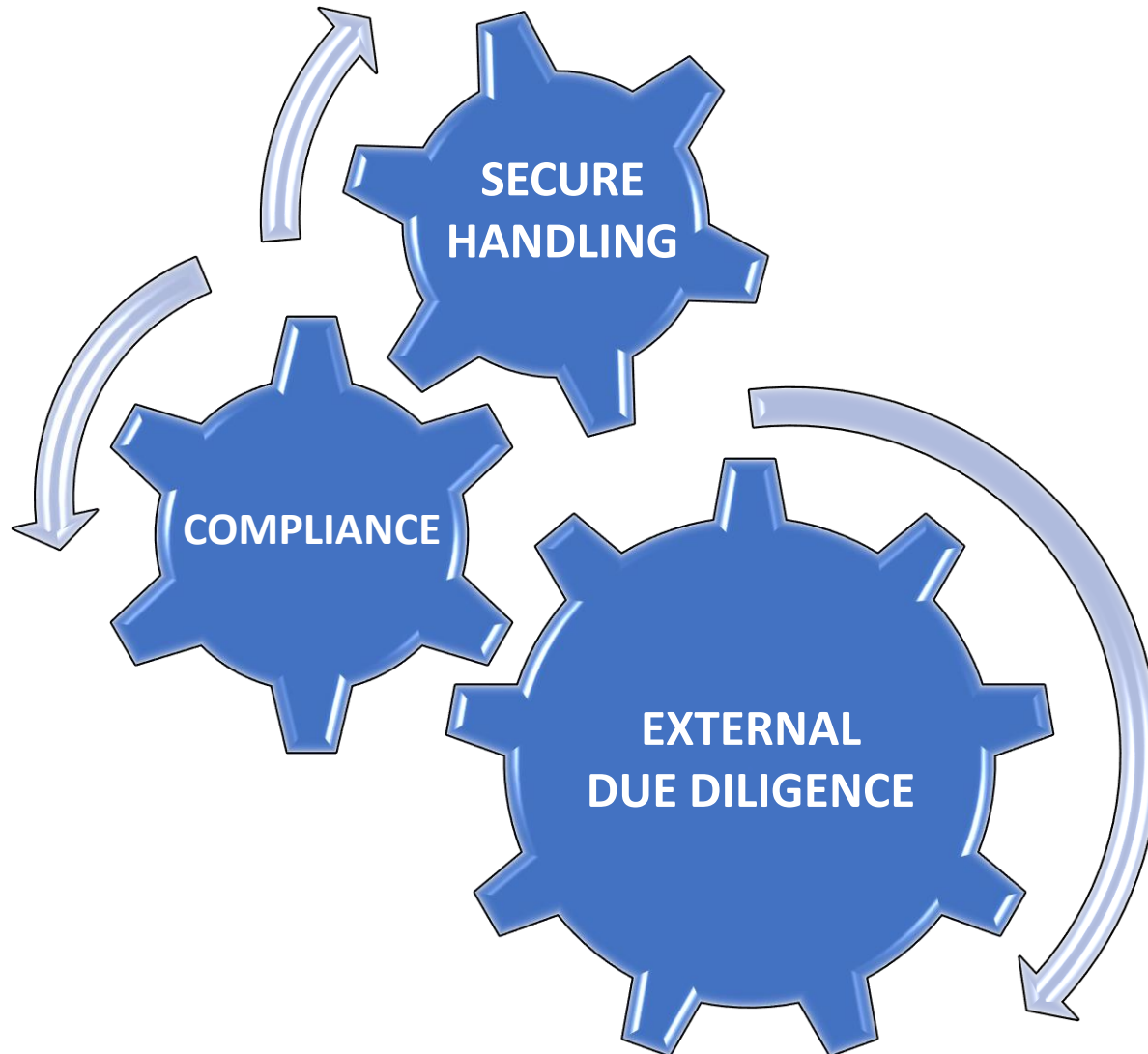**DATA CLASSIFICATION**

SELF SERVE

"AT THE SOURCE"

ACCESS CONTROLS

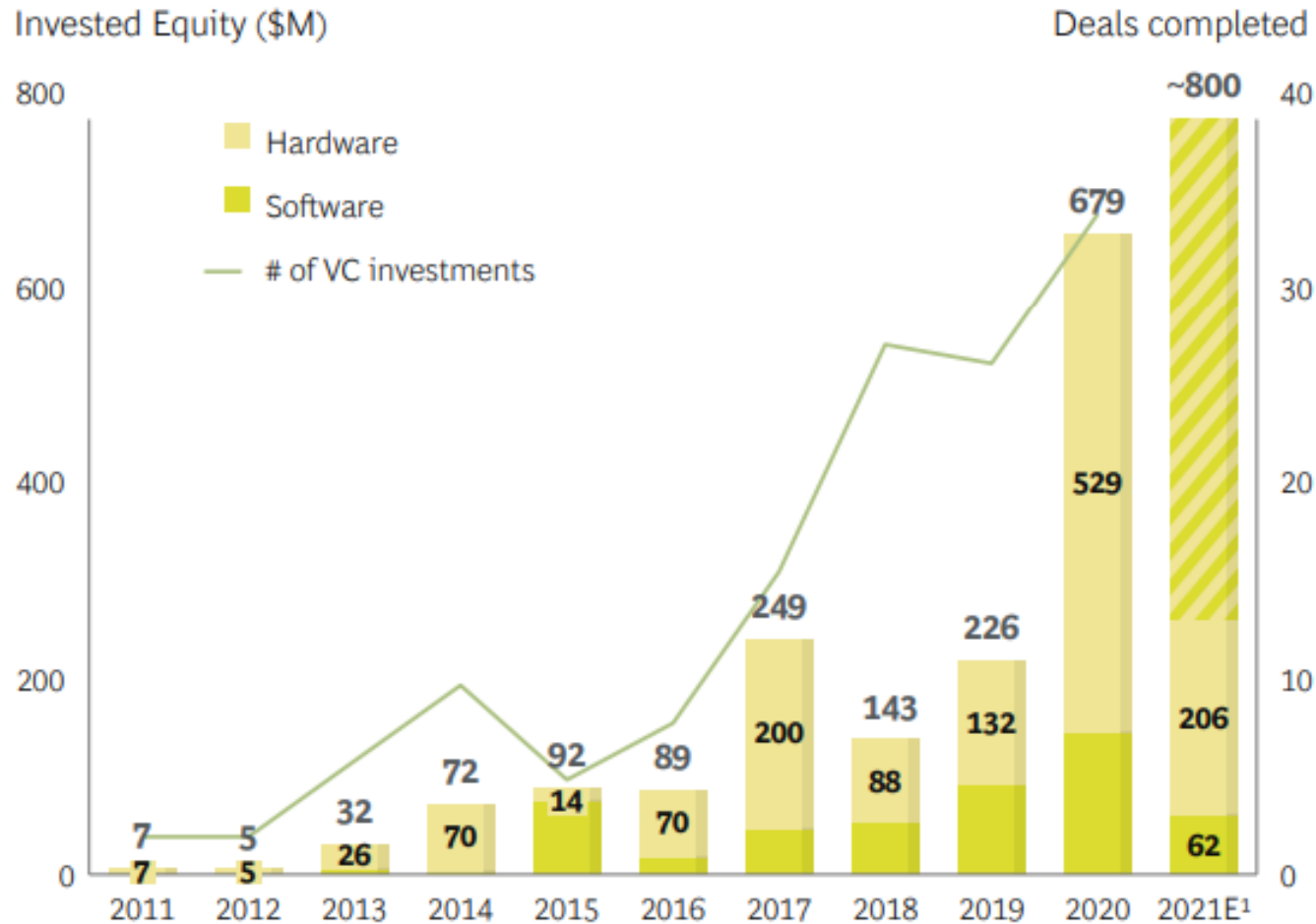**USER EXPERIENCE**

DATA PROTECTION

Data & Cyber: Strategic Business Advantage

- ✓ RFx FLASHCARD
- ✓ NEW BUSINESS WINS
- ✓ CYBER COVERAGE SAVINGS
- ✓ DATA OPERATIONS SAVINGS
- ✓ IT OPERATIONS SAVINGS
- ✓ CYBER SAVINGS
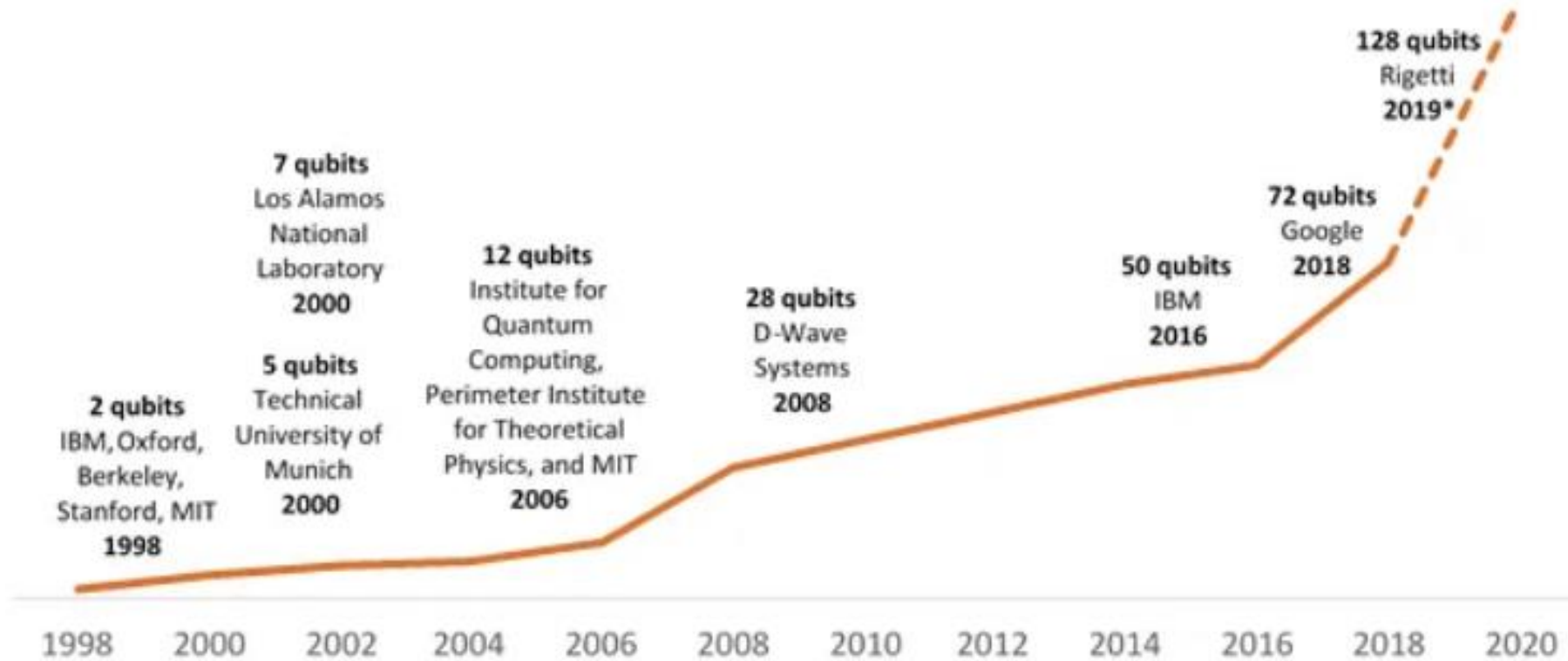- ✓ CERTIFICATIONS
- ✓ COMPETITIVE ADVANTAGE

SECURE HANDLING

COMPLIANCE

EXTERNAL DUE DILIGENCE

Quantum Computing: Significant Investment Growth Recently

Source: Boston Consulting Group

Quantum Computing: Remarkable Growth of Achieved Qubits

128 qubits
Rigetti
2019*

72 qubits
Google
2018

7 qubits
Los Alamos
National
Laboratory
2000

12 qubits
Institute for
Quantum
Computing,
Perimeter Institute
for Theoretical
Physics, and MIT
2006

50 qubits
IBM
2016

5 qubits
Technical
University of
Munich
2000

28 qubits
D-Wave
Systems
2008

2 qubits
IBM, Oxford,
Berkeley,
Stanford, MIT
1998

1998 2000 2002 2004 2006 2008 2010 2012 2014 2016 2018 2020

Source: FairView Capital

Quantum Computing: Y2Q Timeline TBD

~15 years

- 2,048 RSA bit encryption key length - 2016 NIST recommendation

- 8 hrs to factoring 2,048 bit RSA integers using only 20 million physical qubits

- Plans to build quantum computer with 1 million physical qubits by 2030

- Recently discovered topological quantum - more stable and more scalable

Quantum Computing: Clear Trajectory

Quantum Computing: Risks & Opportunities

$$$
Difficult to build & require unique components, expensive tech and massive cooling

SPEED
Quantum computers are so fast that classical digital computers can never match

POTENTIAL ERRORS
Depending on the nature of qubits and quantum mechanics, errors are possible

SOLUTION POTENTIAL
No matter how complex the problem is, quantum computing allows

TARGETED TASKS
Quantum computers have the potential to find revolutionary solutions, but only in specific areas and for specific tasks

SOLUTION COMPLEXITY
Given the complexity and speed that quantum computing can achieve, quantum computers can run complex simulations

Quantum Potential Use Cases: It's All About DATA

ENCRYPTION

DATA ANALYTICS

PATTERN MATCHING

DECISION OPTIMIZATION

FORECASTING & PREDICTIONS

CYBERSECURITY

RESEARCH & DEVELOPMENT

AVIATION & AEROSPACE

AUTOMOTIVE

CYBER THREATS

Quantum Computing: Key Considerations to Crypto Agility

- Encrypted data stolen
- May still be unencrypted for now
- Quantum computing decryption is a matter of time

LOOMING THREAT

- Quantum-secure takes time: multi-step journey
- Data
- Tooling
- Infrastructure
- Policies
- Training

PREPARATION JOURNEY

- Canada: Guidance on becoming cryptographically agile - ITSAP.40.018 (05'22), Preparing your organization for the quantum threat to cryptography - ITSAP.00.017 (02'21)
- US: the Quantum Computing Cybersecurity Preparedness Act is Law H.R. 7535 (12.22.2022)
- Encouragement to adopt technology protecting against quantum computing attacks

QUANTUM LAW

Crypto Agility: Data is Key

Crypto Policies: enterprise-wide awareness & requirements

Shared Responsibility: collaboration & delegation

Central 'Organization': governance, tools, guidance

Procurement Policy: crypto agility go forward

New IT Change Management Policies:
- Ongoing inventory maintenance,
- Configuration change management

New Frameworks:
- Incident response
- Software layer for APIs
- Application development
- Secure update mechanisms

Inventory: products that use cryptography

Recommended Standardized Crypto Algorithms: ITSP.40.111 and ITSP.40.062

Transition Plan: non-agile products / legacy cryptography to upgrade to crypto agile products

Crypto Algorithms Validation under Cryptographic Module Validation Program

Crypto Products **Vendor / 3rd Party Review**:
- Support for crypto agility
- Software / firmware upgrade policies
- Required crypto agility updates

Data Awareness: Foundation to Quantum-Proof Tomorrow

CENTRALIZED VISIBILITY
Data. Crypto products. Roles. Data classification, access, residency. Data protection controls.

OWNERSHIP
Appropriate teams / groups and suitable duties

ACTIVE RESPONSIBILITY
Awareness. Agreement. Operationalization.

COMPLIANCE
Defined accountability. Industry practices. Legislative guidance. Corporate standards.

DATA GOVERNANCE
Comprehensive current meta data. Clear scope: sensitive, confidential, business, personal, etc.

THIRD PARTIES
Contracts. Provisions. Disclosures. Roadmaps. SLA's. Standards. Audits.

PROACTIVE CYBER RESILIENCE
Data access framework. Need to know. Role based access. Control posture. Threat awareness. DLP. Preemptive 3rd party assurance

RESOURCING
Sufficient & knowledgeable. Crypto & governance experience. Training.

VULNERABILITIES
Full lifecycle management and proper SLA's

THE LATEST
Crypto techniques, algorithms, technology. High bits sizes.

HARDWARE
Updates, upgrades and patches OR switch

MONITORING & REPORTING
Products and roles. Crypto libraries, keys, key mgmt. systems. Ongoing ownership tracking. Maintenance. Reporting.

AUTOMATION
Where suitable: management and replacement tracking

Data & Cyber Partnership: Key Takeaways

- ➢ **COMPETITIVE ADVANTAGE**

- ➢ **QUANTUM: WHEN, NOT IF**

- ➢ **CRYPTO AGILITY: DATA IS KEY**

- ➢ **ONGOING SYNERGY IS SUCCESS**

Thank You

Natalia Bakhtina, MBA
LinkedIn

Questions and Answers