Securing The Future With Quantum-Safe Solutions

Mike Brown, CTO of ISARA Corp.

October 2017


Quantum computing will solve today's unsolvable problems, opening up
A NEW REALM OF POSSIBILITIES.
ISARA


THE "QUANTUM"
RACE IS ON
Microsoft
Google
rigetti
IBM
D:Wave
The Quantum Computing Company™
intel
ISARA


THE CHALLENGE
Quantum computing will break today's public key encryption standards.
ISARA

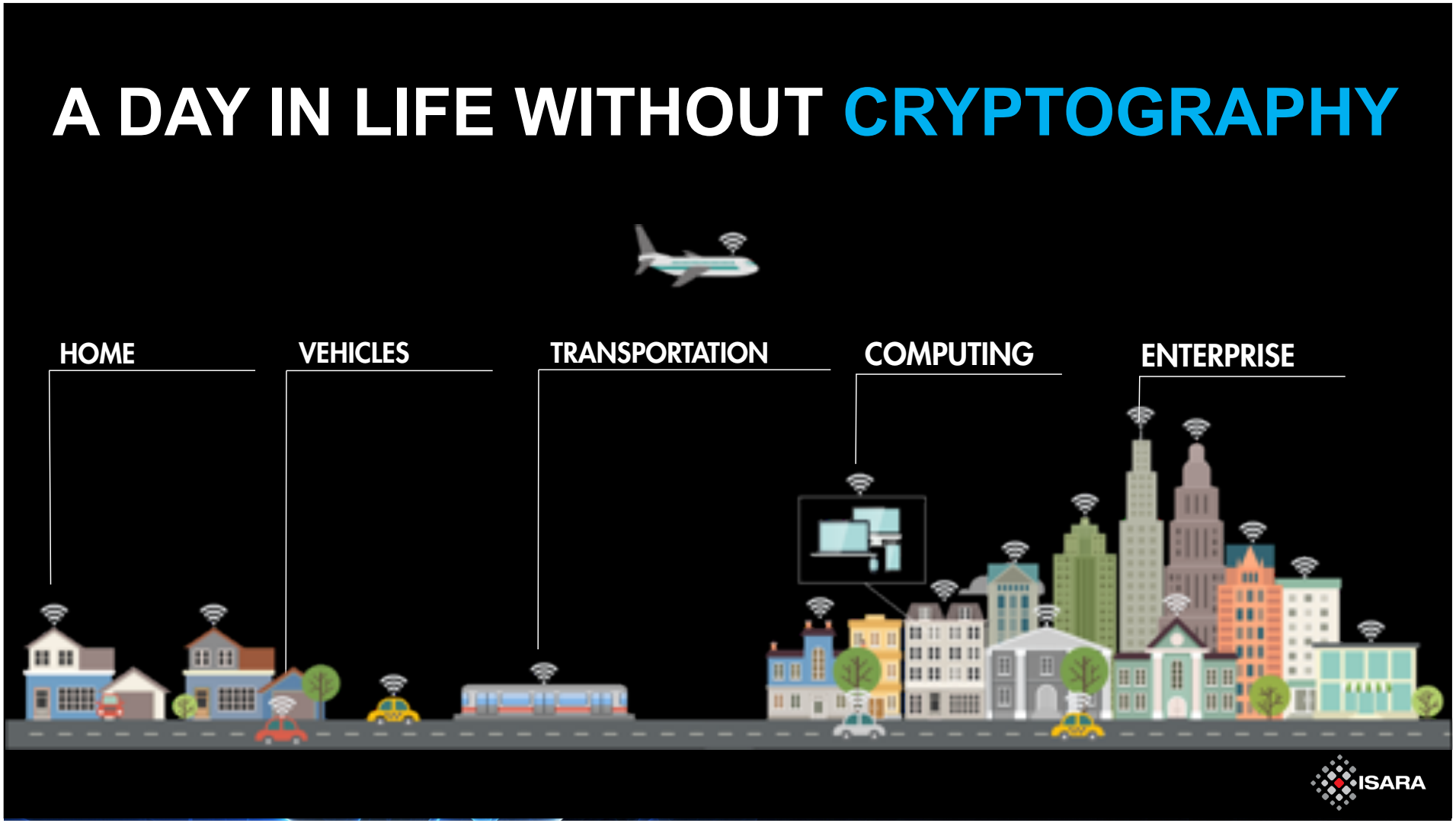

QUANTUM COMPUTING WILL PUT AT RISK
Confidentiality
Roots of Trust
Identity Management
ISARA

TIMELINE TO QUANTUM CHALLENGE:

2026

ISARA

A DAY IN LIFE WITHOUT CRYPTOGRAPHY



THE COST OF DATA BREACHES CONTINUE TO RISE

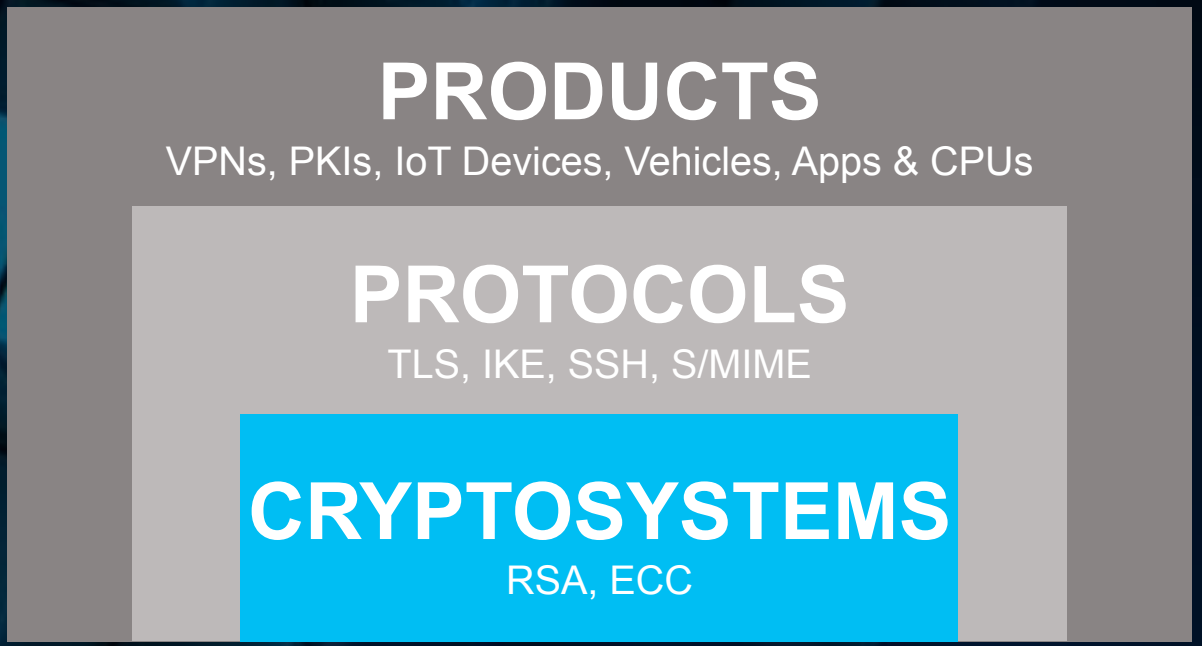
Global Average Cost Per Incident

$4M

⬆29% since 2013

ISARA

WHAT'S VULNERABLE?



ISARA

QUANTUM-SAFE CONSIDERATIONS

- Life of your secrets
- Threat horizon
- Ability to integrate tools
- Upgrade costs
- Value of your assets
- Key infrastructure
- Critical technologies

ISARA


SUCCESS IS A
SEAMLESS
(and cost effective)
MIGRATION
…with no impact to end user experience.
ISARA

PATHWAYS TO QUANTUM SAFETY

Quantum Key Distribution (QKD)

Quantum Random Number Generation (QRNG)

ISARA

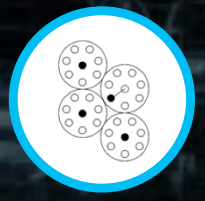
Quantum-Safe Cryptography

THE "NEW" MATH

Hash-based signatures

Isogeny-based

Multivariate-based



Code-based

Lattice-based

ISARA


SUCCESS REQUIRES
STANDARDS
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce
ETSI
IETF
Accredited Standards
Committee X9 Inc.
Financial Industry Standards
ISO
ITU
ISARA

NEXT STEPS…

Start now.
Identify secrecy obligations.
Start prototyping.
Engage vendors.
Consider the long-term.


QUANTUM-SAFE
The next generation
of cybersecurity
ISARA

ISARA's SOLUTIONS

RADIATE SECURITY SUITE

Optimized library of quantum-safe algorithms and migration tools.

PROFESSIONAL SERVICES

Architecture and design
Migration planning
Custom Implementation
Contract Research

LICENSING

Custom licensing for OEM's and Security Solutions Developers

TESTING & PILOTING

Full end to end test environment
Pilot set-up and monitoring

ISARA

CLEARING THE PATH TO QUANTUM-SAFE SECURITY

www.isara.com
quantumsafe@isara.com

Join us on social

@ISARACorp @ISARACorp @ISARA Corporation

ISARA


ISARA