Crypto Agility

Adapting and Prioritizing Security in a Fast-Paced World

Chujiao Ma, PhD

Security R&D Engineer

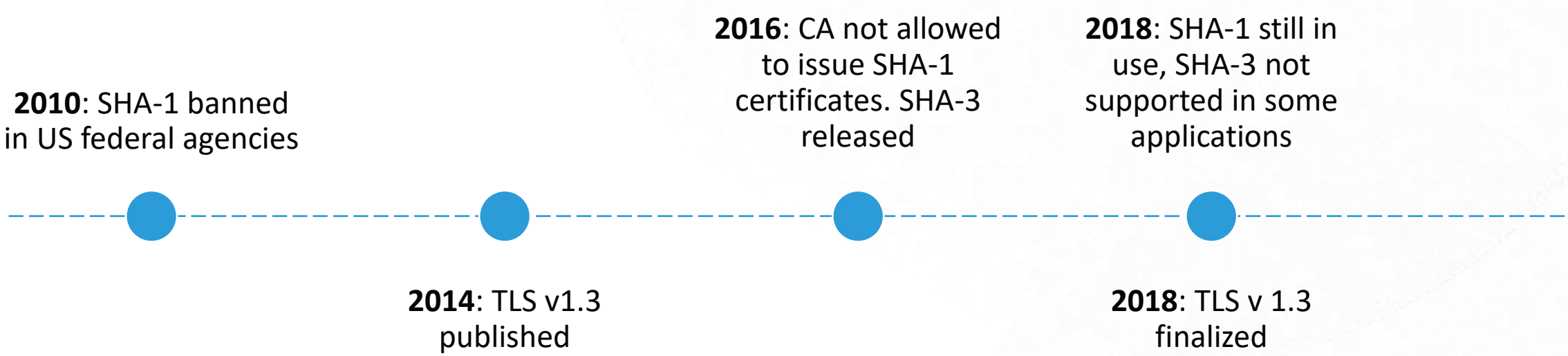
Comcast Cable

June 3, 2021

COMCAST

CHANGE IS INEVITABLE

Crypto-agility: the ability to replace crypto primitives, algorithms, or protocols with limited impact on operations and with low overhead.



COMCAST

CRYPTO AGILITY NOW

Transition can be a long and difficult process

- Algorithms are expected to last decades
- Certificates etc will be used by many relying parties
- Some assets may not be able to support new algorithms

Proactive

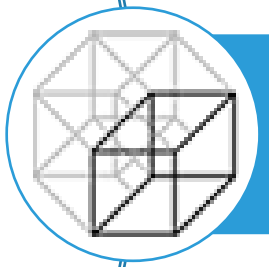
~~**Reactive**~~

COMCAST

EXISTING SOLUTIONS

Senetas CN Series Hardware Encryptors

Flexible FPGA architecture that enables in-field upgrades



Cryptomathic Crypto Service Gateway 3.10

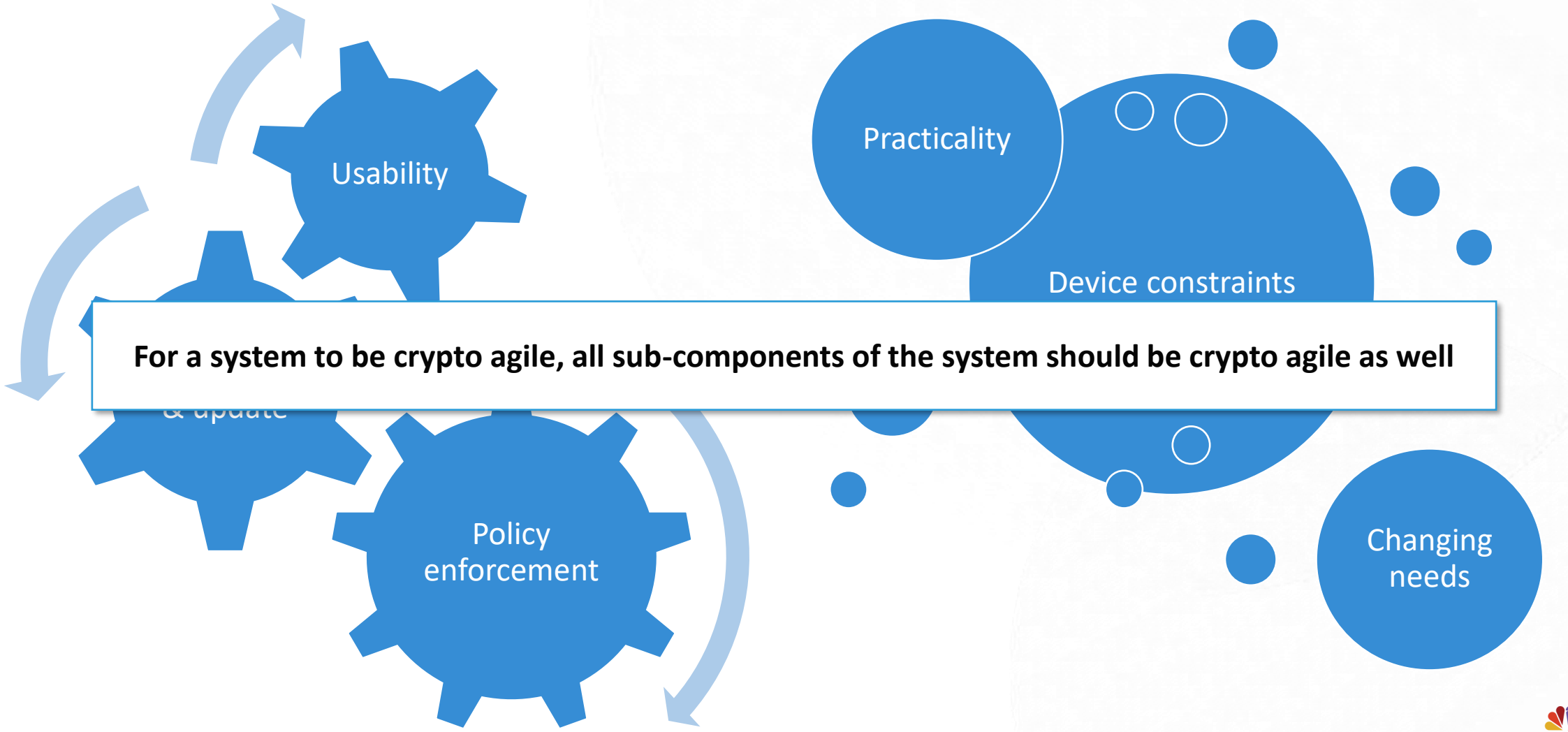
Cryptographic control center that acts as a HSM service and crypto policy management interface

InfoSec Global’s AgileSec Multi-Crypto platform security system

End points cryptographic toolkit and management server infrastructure that deploys and sets policy

COMCAST

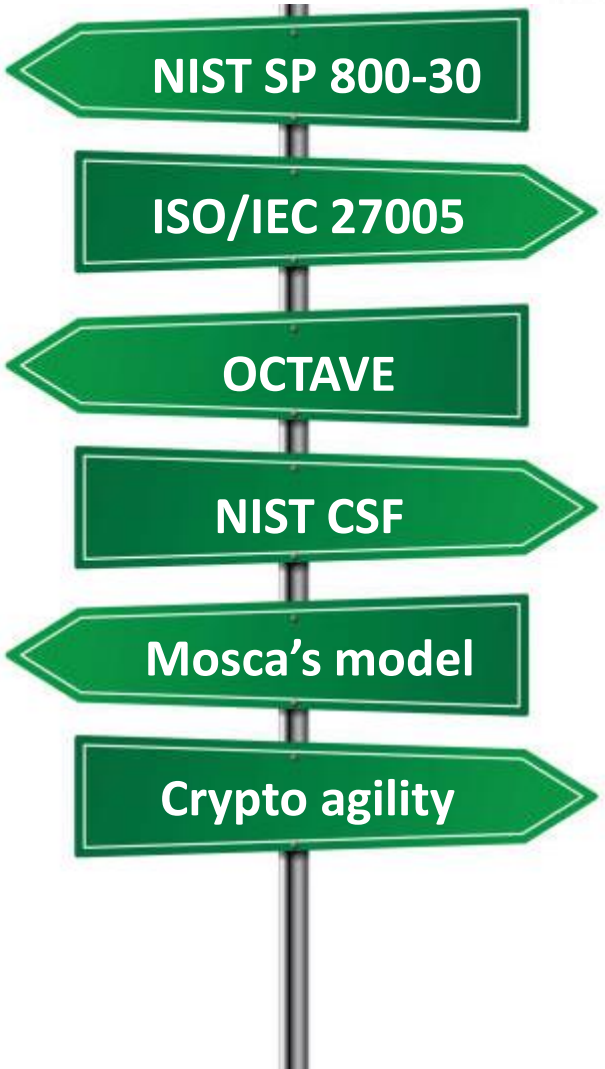
CONSIDERATIONS



For a system to be crypto agile, all sub-components of the system should be crypto agile as well

COMCAST

RISK ASSESSMENT FRAMEWORKS



focuses on risk of technology

focuses on information security

focuses operational and organizational view

focuses on known threats

focuses on risk from quantum timeline

……?

COMCAST

CARAF

Crypto Agility Risk Assessment Framework

CARAF

Crypto Agility Risk Assessment Framework

Towards a realistic framework optimized for quick response

Phase 1: Identify threats

Phase 2: Inventory of assets

Phase 3: Risk estimation

Phase 4: Secure assets through risk mitigation

Phase 5: Roadmap

COMCAST

PHASE 1 – IDENTIFY THREAT

Policy requirements	Governmental, company-wide Usually includes guidelines and timelines
Newly discovered vulnerabilities	Time critical depending on impact Can learn from existing case studies
Disruption from new technology	No concrete timeline No prior instances of transition

COMCAST

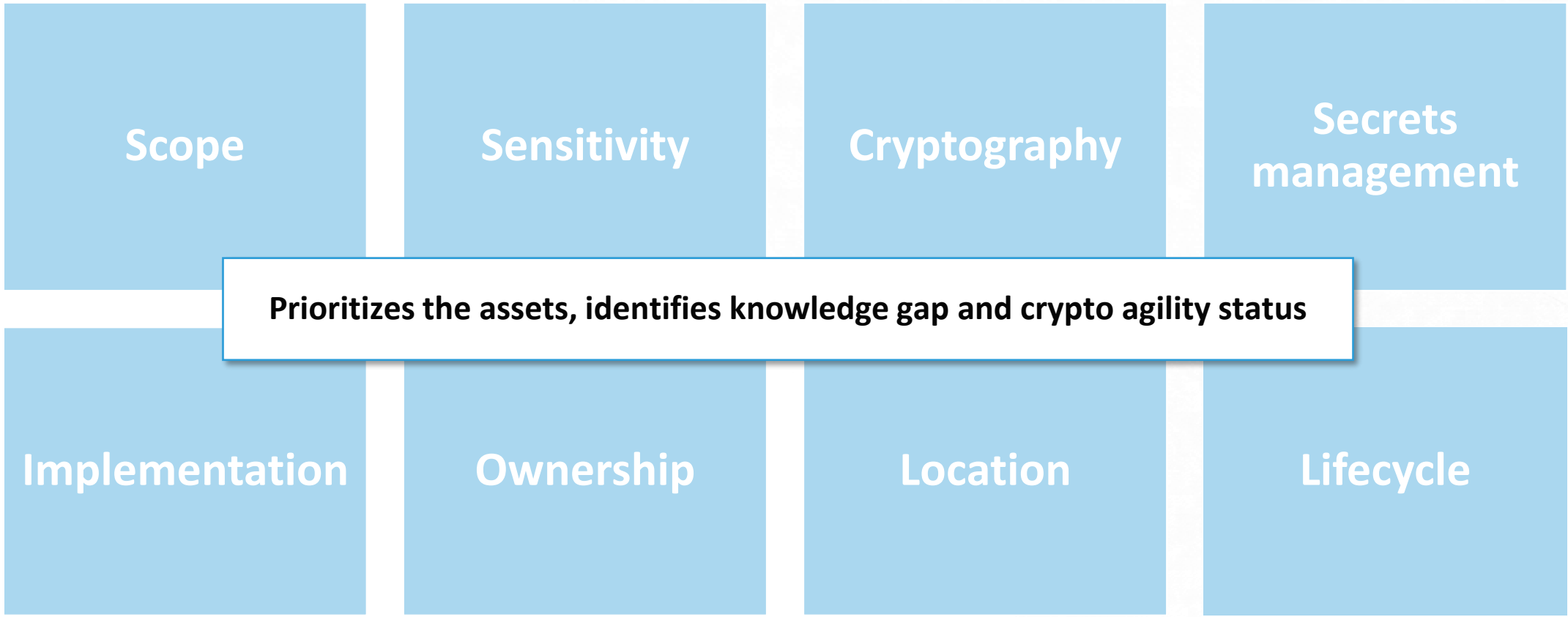
PHASE 2 – INVENTORY OF ASSETS

Factors to consider for each type of assets:

Scope	Sensitivity	Cryptography	Secrets management
Implementation	Ownership	Location	Lifecycle

COMCAST

PHASE 2 – INVENTORY OF ASSETS



COMCAST

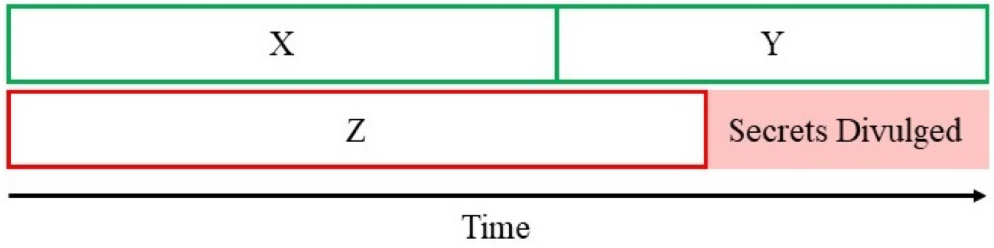
PHASE 3 – RISK ESTIMATION (TIMELINE)

~~RISK = PROBABILITY * IMPACT~~ RISK = TIMELINE*COST

Timeline

- **X** – remaining lifespan of the asset during which it must be protected
- **Y** – time needed for mitigation and implementation
- **Z** – years before threat results in a compromise

If X+Y>Z, there is a problem



COMCAST

PHASE 3 – RISK ESTIMATION (COST)

Cost will vary depending on the type and design of assets as well as availability of resources

Design consideration

- Implementation independence
- Simplicity
- Flexibility
- Performance

Migration consideration

- Cryptography
- Secrets management
- Implementation
- Ownership
- Location

COMCAST

PHASE 4 – RISK MITIGATION

PHASE OUT

When the value of the asset is lower than the expected risk

ACCEPT THE RISK

When the value of the risk is lower than organization's risk tolerance

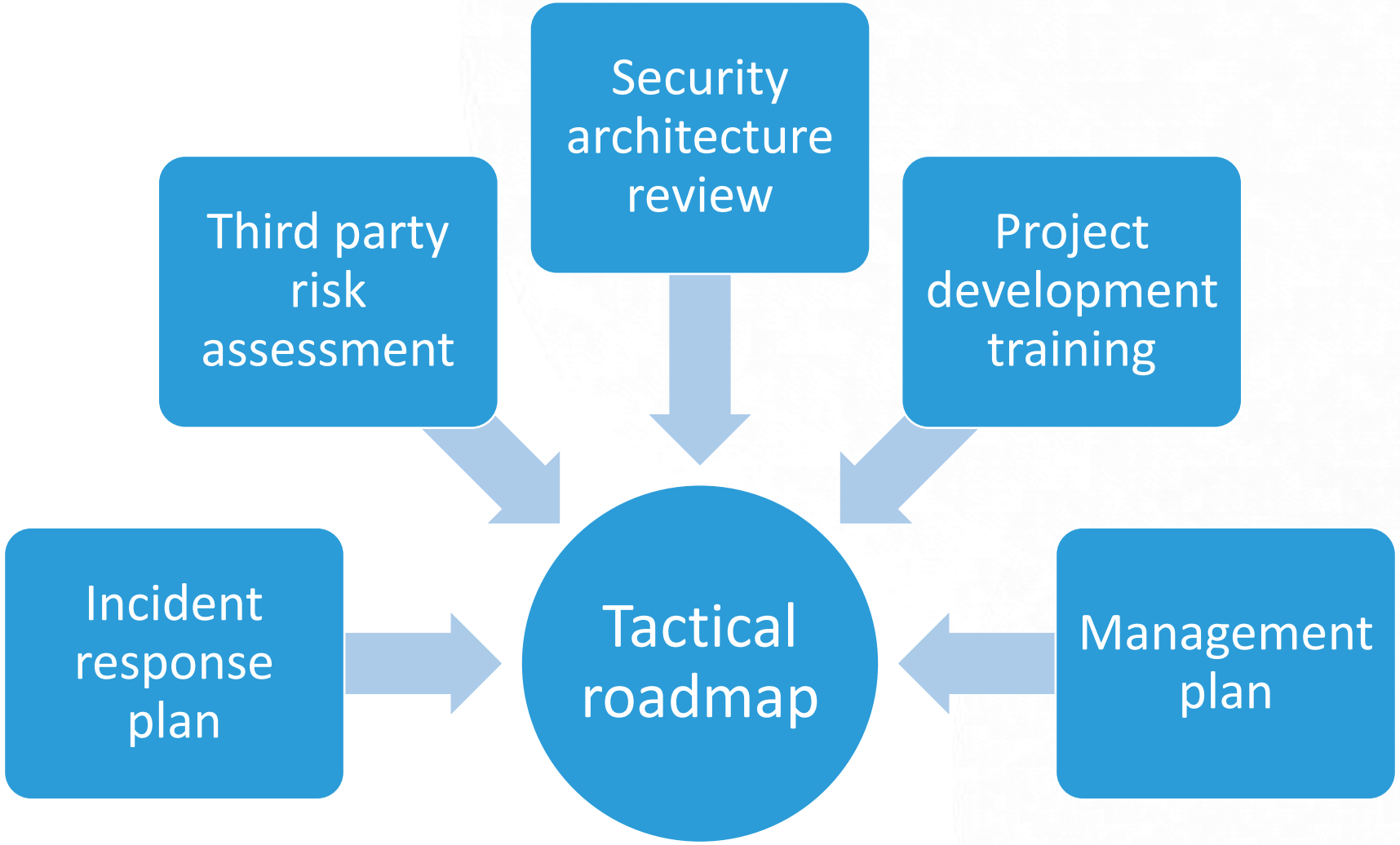
SECURE THE ASSET

When the value of the asset is greater than the cost to secure it.

	Low Cost	High Cost
X + Y < Z	Phase Out	Accept Risk
X + Y > Z	Secure Asset	Phase Out

COMCAST

PHASE 5 – ORGANIZATIONAL ROADMAP



COMCAST

USE CASE

Quantum Computing

1. IDENTIFY THREAT - QUANTUM

NIST is currently in the final round of Post-Quantum Cryptography competition. The selected algorithms will "supplement or replace standards considered to be most vulnerable to a quantum attack"

- FIPS 186-4
- NIST SP 800-56A
- NIST SP 800-56B

COMCAST

2. INVENTORY OF ASSETS

Cryptographic Algorithm	Type	Purpose	Impact
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	Hash	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECC	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field)	Public key	Signatures, key exchange	No longer secure

NIST Report on Post-Quantum Cryptography

What's affected

- IoT devices
- Assets using TLS
- High value, high shelf life data (Ex. Social security number)

COMCAST

3. RISK ESTIMATION - TIMELINE

Risk = Timeline*Cost

Timeline Risk (X + Y > Z)	1- low	2- medium	3- high	4 - critical
X (shelf-life)	0 – 5	6-10	11-20	20+
Y (mitigation)	0 – 5	6-10	11-20	20+
Z (threat)	20+	10-20	5-10	0 – 5

- Blackberry took **5 years** to move from 3DES to AES. They are in control of all devices and servers.
- A survey of experts showed that 90% think there is more than 50% likelihood of quantum becoming a significant threat to public-key cybersecurity **in 20 year**, with 22% indicating it would be > 95%.
- NIST posits that a quantum computer capable of breaking 2000-bit RSA in a matter of hours could be built by **2030** for a budget of about a billion dollars.

COMCAST

3. RISK ESTIMATION - COST

Risk = Timeline*Cost

Asset Type (Support for PQC)	1 – Low risk	2 – Medium risk	3 – High risk	4 – Critical
Enterprise (Support)	Medium	Low	Low	Low
Enterprise (No support)	High	High	Medium	Medium
Third Party (Support)	High	High	Medium	Low
Third Party (No support)	High	High	High	High

- The exact value of the migration will differ based on the organization, the type of IoT asset etc.

COMCAST

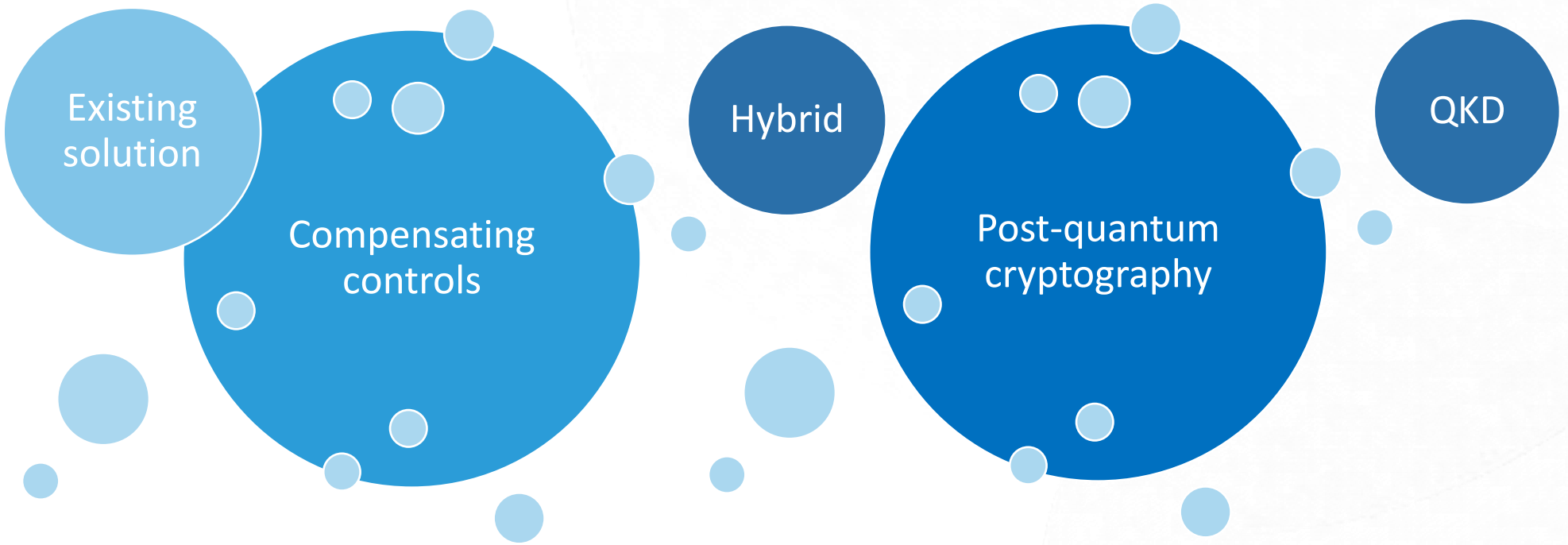
4. MITIGATION STRATEGY

Mitigation based on the risk and level of support

Asset Type (Support for PQC)	1 – Low risk	2 – Medium risk	3 – High risk	4 – Critical
Enterprise (Support)	Accept Risk + Phase Out	Secure	Secure	Secure
Enterprise (No support)	Accept Risk + Phase Out	Accept Risk	Secure + Phase Out	Secure + Phase Out
Third Party (Support)	Accept Risk + Phase Out	Accept Risk	Secure + Phase Out	Secure + Phase Out
Third Party (No support)	Accept Risk + Phase Out	Accept Risk	Phase Out	Phase Out

COMCAST

4. SECURE ASSETS



COMCAST

5. ORGANIZATIONAL ROADMAP

Accept risk	• Continue enforcing existing management plans • Include an exception process for the assets in question
Phase out	• Review alternative solutions and include requirements around post-quantum security in the guidelines
Secure asset	• Benchmark test which PQC is appropriate for the asset • Upgrade to quantum safe alternatives

COMCAST

NEXT STEP

There are a lot of work to do

Be realistic about short term but optimistic about long term

Act now!

Recommendations

- Current and thorough inventory of cryptography and products involved
- Incorporate crypto agility into the development, workflow and assessment
- Active monitoring of current and potential threats

Thank You!

Reference

(Accepted) Chujiao Ma, Luis Colon, Joe Dera, Bahman Rashidi and Vaibhav Garg. “CARAF: Crypto Agility Risk Assessment Framework.” *Journal of Cybersecurity*.

Contact info

- chujiao_ma@comcast.com
- https://www.linkedin.com/in/chujiao-ma/


COMCAST