Crypto Agility Risk Assessment Framework (CARAF)

Bahman Rashidi,

Senior Director, Cybersecurity & Privacy Research Engineering

A BRIEF HISTORY

1982
- Feynman proposes computation based on quantum mechanics

1994
- Peter Shor proposes a quantum factoring algorithm

1996
- Lov Grover proposes a quantum search algorithm

2011
- D-Wave sells the first commercially available quantum computer

2016
- NIST Launches the PQC Standardization Effort

2021
- Biden EO on emphasizes the need for stronger encryption including transition to PQC

2022
- NSA updates CNSA to 2.0 including quantum resistant algorithms

2023
- NSM-10 directs federal agencies to begin preparing for transition to PQC

2024
- NIST releases first set of FIPS for PQC

2025: NIST selected the 5th algorithm for general encryption.

TRANSITION WE MUST

CRQC

Timeline Unknown

- The timeline for a **cryptographically relevant quantum computer** is unclear.
- Most estimates indicate that **Q-Day** is 15 years away.

US Government

Timeline → 2035

- Transition from current crypto systems by 2030.
- Complete deprecation of algorithms by 2035.

Necessity

Timeline → Now

- Harvest Now, Decrypt Later
- Prolonged migration
  - DES → AES~10yrs
  - SHA1 → SHA2 +10yrs

CRYPTO AGILITY

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

CARAF

CRYPTO AGILITY RISK ASSESSMENT FRAMEWORK

Phase 1:
Identify Threats

Phase 2:
Inventory of Assets

Phase 3:
Risk Estimation

Phase 4:
Risk Mitigation

Phase 5:
Roadmap

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

PHASE 2 – INVENTORY OF ASSETS

Factors to consider for each type of assets:

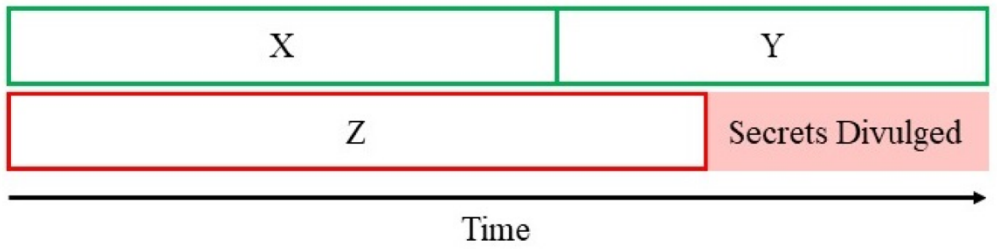
Scope	**Sensitivity**	**Cryptography**	**Secrets management**
Implementation	**Ownership**	**Location**	**Lifecycle**

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



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

PHASE 4 – RISK MITIGATION

PHASE OUT

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

ACCEPT THE RISK

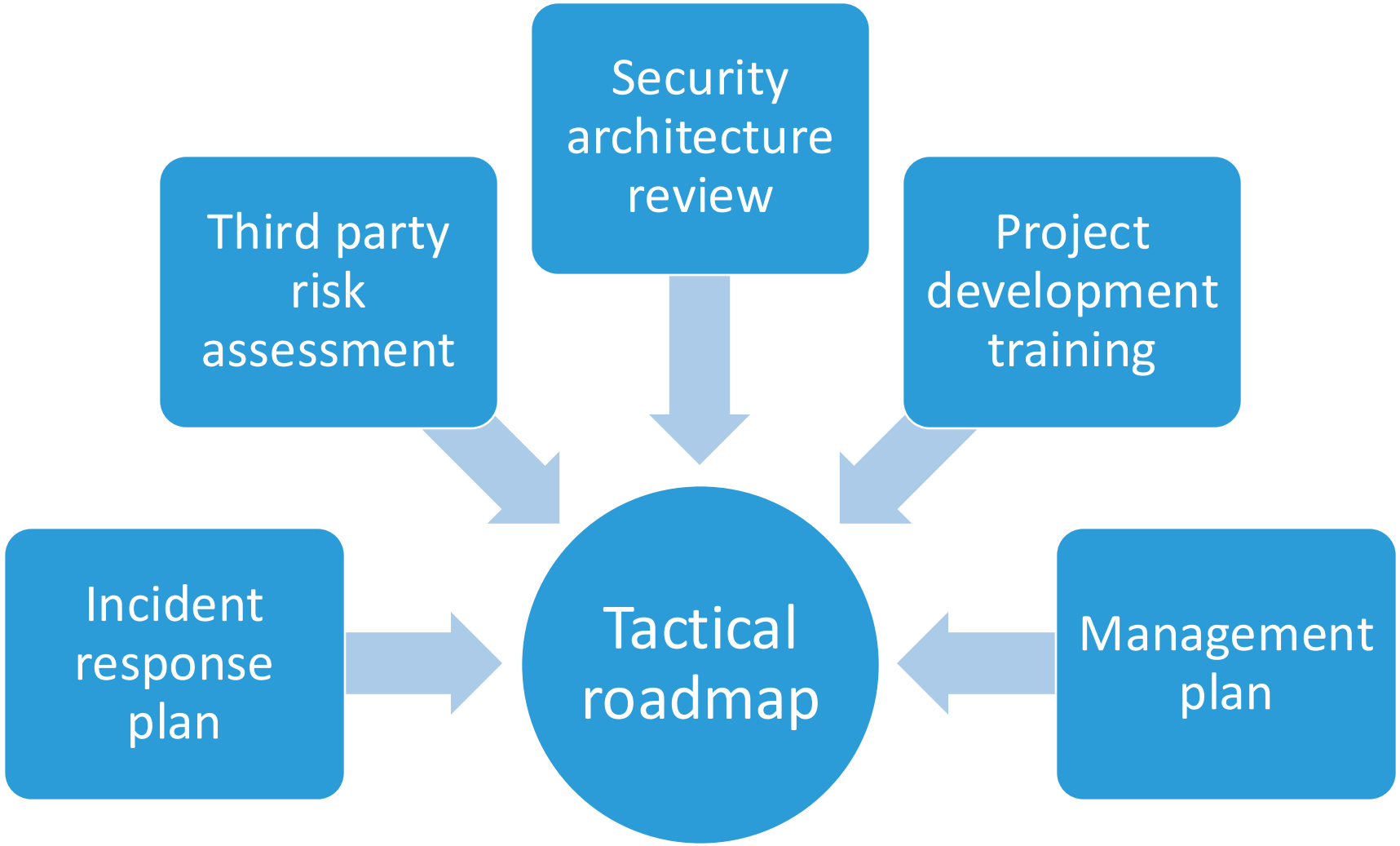
When the value of the risk is lower than organization's risk tolerance

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

PHASE 5 – ORGANIZATIONAL ROADMAP



Thank you!

Bahman Rashidi, PhD
Senior Director, Cybersecurity & Privacy Research Engineering
Comcast Cable

bahman_Rashidi[at]comcast.com
LinkedIn