DNV
CYBER

Practical PQC Migration

Part 1 – Understanding the risks of PQC and urgency of migration

Tor Helge Kristiansen, DNV Cyber

28 October 2025

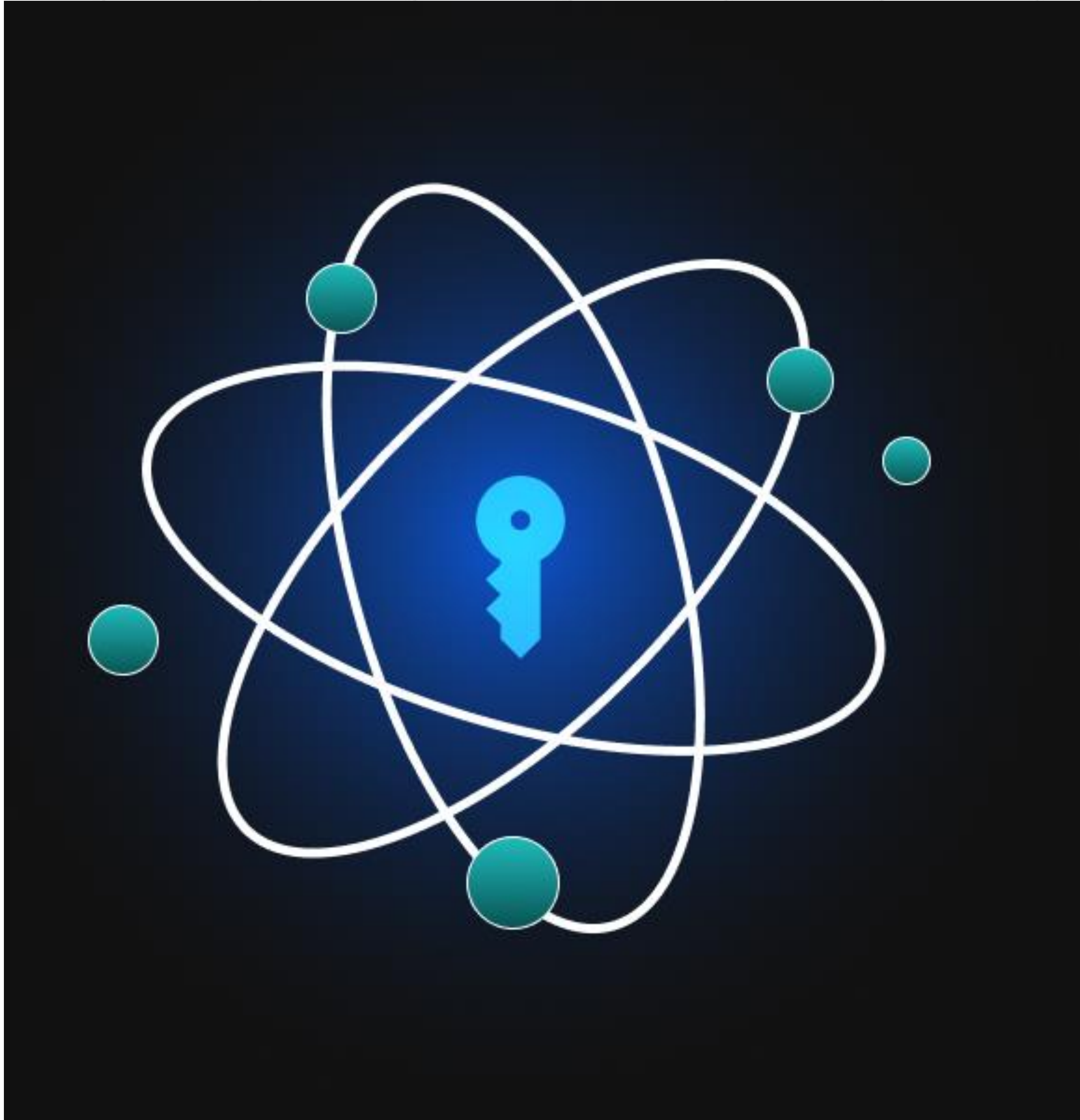
Agenda

01 Introduction to PQC Migration

02 Preparation

03 Establishing Baseline Understanding

04 Group Exercise



Introduction to PQC Migration

Why do we care about Cryptographically Relevant Quantum Computers (CRQC)?

CRQC will be able to easily crack current asymmetric cryptographic algorithms

- Effectively rendering our systems which secure communications, ensure authenticity, and protect sensitive data, unusable
- A CRQC computer is likely 10 to 20 years away
- At this point, all our security systems must be based on quantum-safe cryptographic algorithms (PQC)

The “Harvest Now, Decrypt Later” threat makes this PQC migration even more urgent

- Adversaries are actively collecting vast quantities of currently encrypted data, with the explicit intent to decrypt it when CRQC becomes available

- This transforms what might appear as a distant quantum threat into an **immediate concern**
- The longer the required confidentiality period for your sensitive data, the higher the urgency to migrate

The “Harvest Now, Decrypt Later“ Threat
PII

PQC migration is a **complex**, **enterprise-wide** transformation deeply interwoven with an organization’s **unique** risk profile, operational realities, and financial constraints

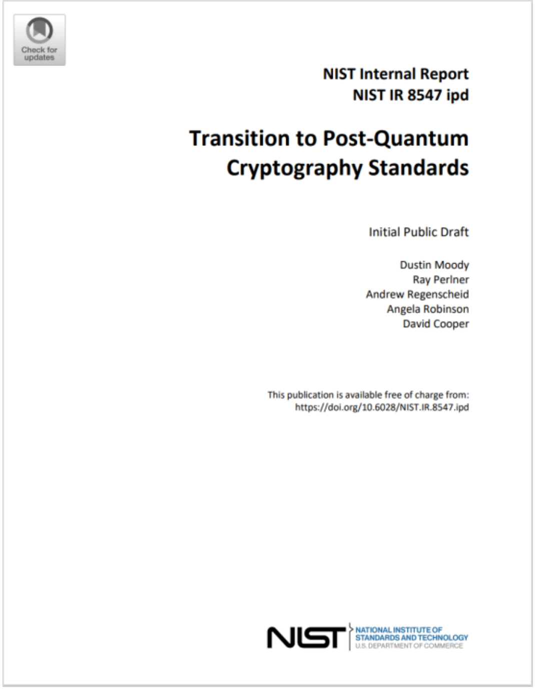
Fortunately, there is some guidance available for how to perform this PQC migration

NSM
SENTER FOR
ANVENDT KRYPTOLOGI

Kvantemigrasjon

Veileder

Veileder i kvanteflytting fra NSM.pdf



Check for updates

NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum
Cryptography Standards

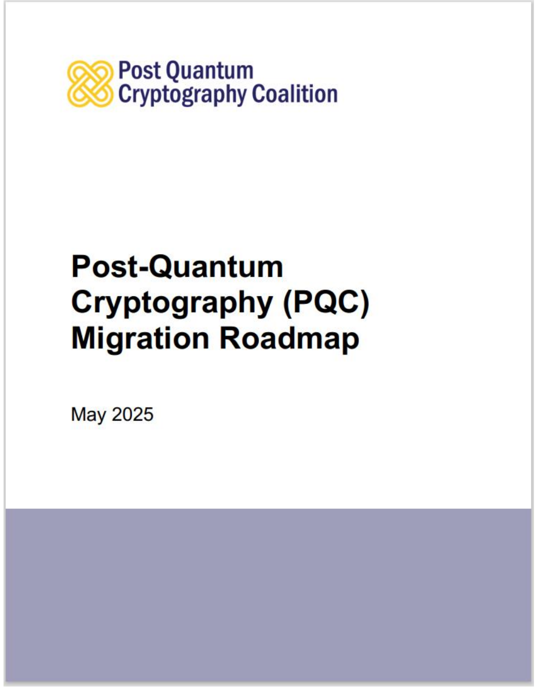
Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8547.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST IR 8547 initial public draft, Transition to Post-Quantum Cryptography Standards

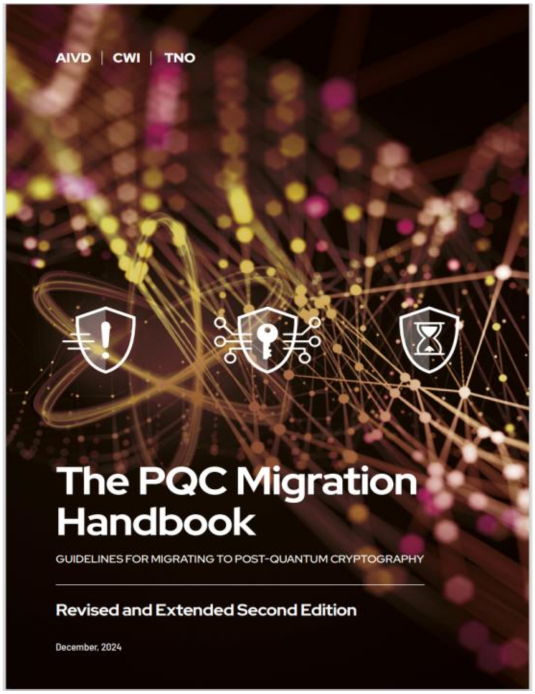


Post Quantum
Cryptography Coalition

Post-Quantum
Cryptography (PQC)
Migration Roadmap

May 2025

PQC-Migration-Roadmap-PQCC-2.pdf



AIVD | CWI | TNO

The PQC Migration Handbook

GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY

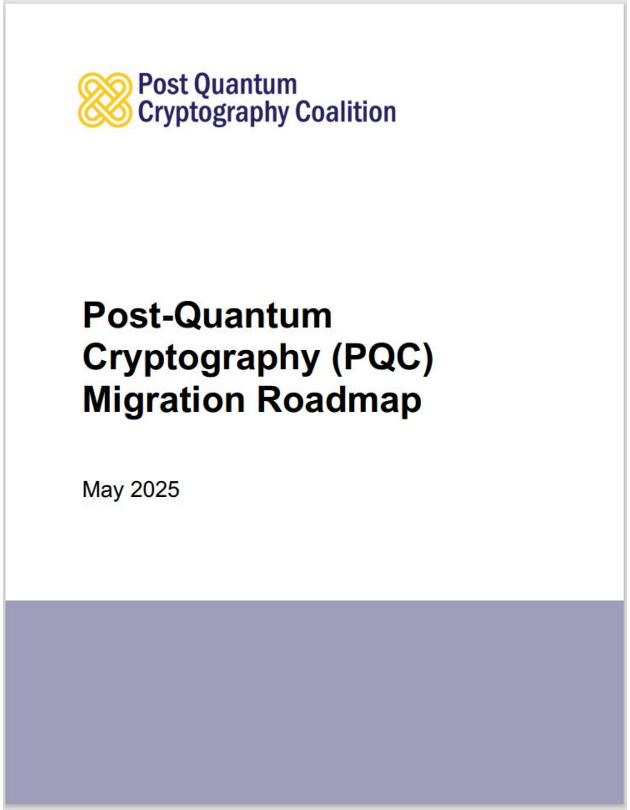
Revised and Extended Second Edition

December, 2024

The PQC Migration Handbook.pdf

DNV
CYBER

Introducing the PQC Migration Roadmap

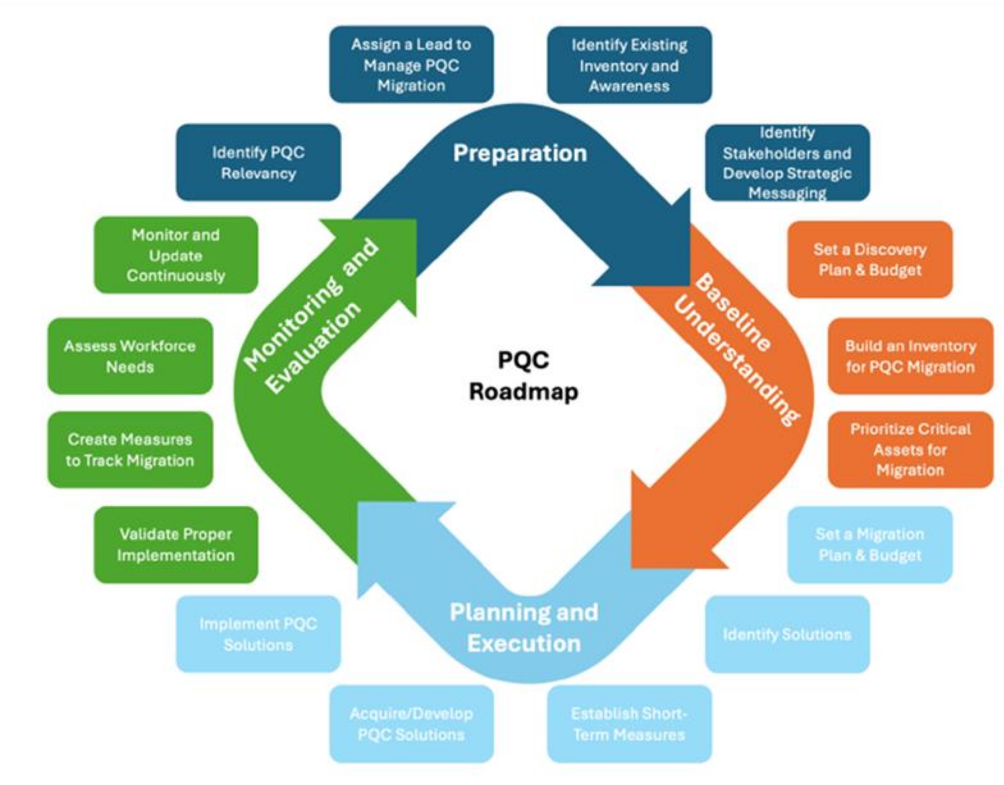


Post Quantum Cryptography Coalition

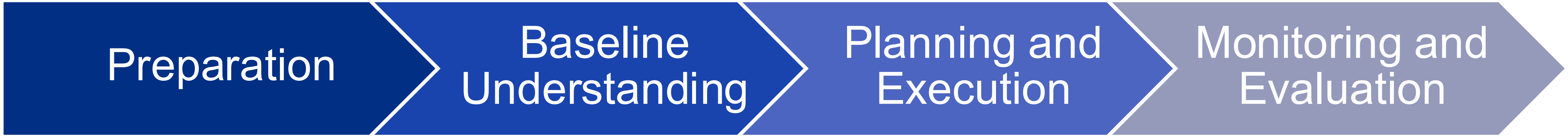
Post-Quantum Cryptography (PQC) Migration Roadmap

May 2025

- Designed to guide organizations through the intricate **process of transitioning** their cryptographic systems to withstand future quantum threats


PQC Roadmap
Preparation
Assign a Lead to Manage PQC Migration
Identify Existing Inventory and Awareness
Identify Stakeholders and Develop Strategic Messaging
Identify PQC Relevancy
Baseline Understanding
Set a Discovery Plan & Budget
Build an Inventory for PQC Migration
Prioritize Critical Assets for Migration
Planning and Execution
Set a Migration Plan & Budget
Identify Solutions
Establish Short-Term Measures
Acquire/Develop PQC Solutions
Implement PQC Solutions
Monitoring and Evaluation
Validate Proper Implementation
Create Measures to Track Migration
Assess Workforce Needs
Monitor and Update Continuously

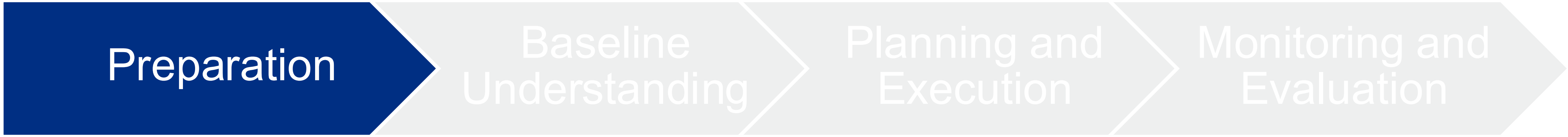
The PQC Migration Roadmap provides a four-phase framework to transition to quantum-safe cryptography



Preparation	Baseline Understanding	Planning and Execution	Monitoring and Evaluation
Obtaining a clear overview of the organization’s PQC migration objectives	Gathering a comprehensive understanding of the organization’s cryptographic landscape	Collaborating with external system vendors and internal system owners to ensure that post-quantum solutions are acquired or developed and implemented effectively	Tracking progress against defined goals and establishing a process for ongoing reassessment of cryptographic security as quantum capabilities evolve

Preparation

Practical PQC migration


Preparation

Baseline Understanding

Planning and Execution

Monitoring and Evaluation

Obtaining a clear overview of the organization's PQC migration objectives	**Gathering a comprehensive understanding of the organization's cryptographic landscape**	**Collaborating with external system vendors and internal system owners to ensure that post-quantum solutions are acquired or developed and implemented effectively**	**Tracking progress against defined goals and establishing a process for ongoing reassessment of cryptographic security as quantum capabilities evolve**
• Identify PQC relevancy • Assign leadership and scope • Identify and engage stakeholders	• Establish or refine data inventory • Develop an inventory of cryptographic assets • Conduct risk assessment and determine urgency	• Select PQC algorithms and solutions • Prepare migration plan • Develop (internal) or acquire (external) solutions • Perform incremental roll-out	• Validate proper implementation • Track migration progress • Review and adapt • Train and prepare staff

Preparation

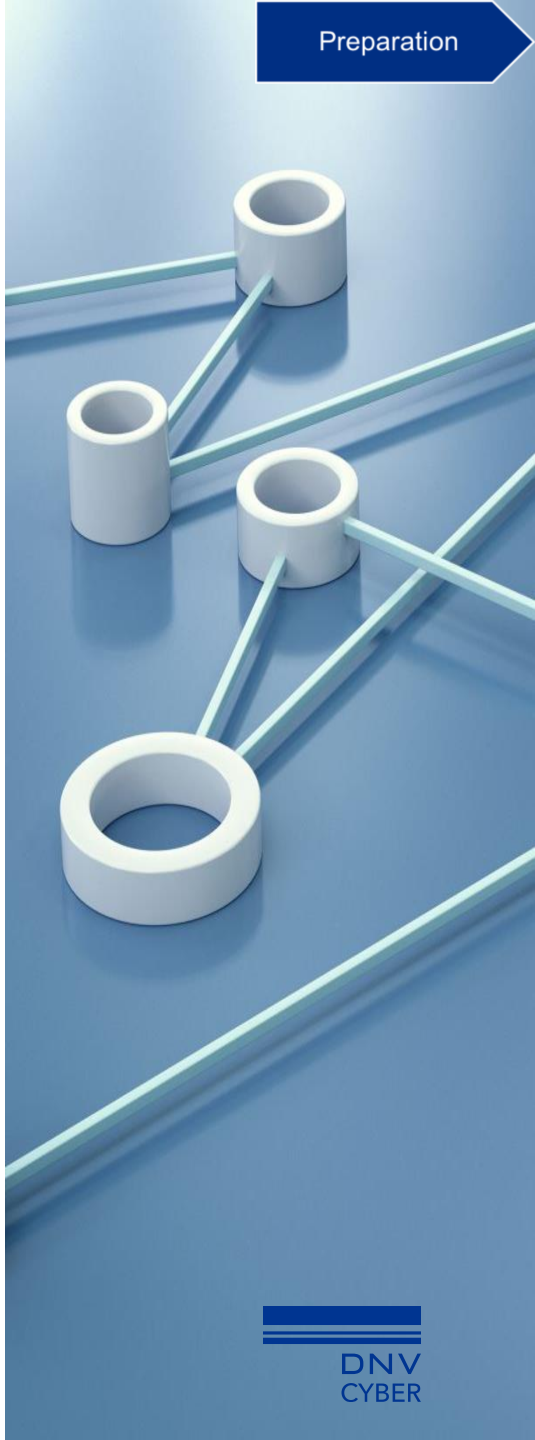
PQC relevancy and urgency of migration depends on type of organization

Cryptography Technology Provider – those that supply cryptographic solutions and services, including infrastructures. Must start PQC migration as soon as possible to support Urgent Adopters.

System Integrators – those that integrate and build systems and solutions that incorporate cryptographic solutions from Cryptography Technology Providers.

Urgent Adopters – those that handle sensitive data or provide critical or long-lived infrastructures; they should start preparing for migration as soon as possible.

Regular Adopters – those that neither handle sensitive data nor provide critical/long-lived infrastructures, or when they do, the risk of an attack by a future quantum computer is manageable.



DNV CYBER

NSM recommends that organizations assess their criticality and urgency based on five factors

Factors:

- The threat level
- The attack surface
- The types of systems and their potential malfunctions
- The criticality and sensitivity of data handled
- The interdependencies with other organizations

Organizations that should consider themselves Urgent Adopters:

- Organizations handling personal data or sensitive data with long lifespan
- Organizations providing or supporting critical infrastructure or long-lived infrastructure

Assign leadership and scope

- Define migration aims to clearly articulate what PQC migration means for your organization
  - Are there any regulatory requirements affecting migration timeline?

- Appoint a senior migration lead (or team) and assign accountability for monitoring and driving the migration
  - Ensure migration lead is well-positioned to coordinate across different areas within and outside the organization
  - Align stakeholders early so the project has authority and resources

- Strategic messaging
  - Communicate the value, purpose, ROI, and resource requirements of PQC migration

Preparation

Engage all key stakeholders early and continuously

- PQC migration involves many internal and external stakeholders – it cannot be siloed into a single IT or security department
- **Internal**: legal, compliance, finance, IT operations, business units, risk management, etc.
- **External**: customers, partners, vendors, cloud providers, regulatory bodies, auditors, etc.

- Recommendations:
  - Begin discussions with internal system operators early to understand operational impact
  - Educate developers, DevOps, and system engineers on upcoming PQC standards
  - Educate legal/compliance since regulations may eventually mandate PQC
  - Begin discussions with external partners and vendors so they know your timelines and can begin their own planning

DNV CYBER

Establishing Baseline Understanding

Practical PQC migration

Preparation	Baseline Understanding	Planning and Execution	Monitoring and Evaluation
Obtaining a clear overview of the organization's PQC migration objectives	**Gathering a comprehensive understanding of the organization's cryptographic landscape**	**Collaborating with external system vendors and internal system owners to ensure that post-quantum solutions are acquired or developed and implemented effectively**	**Tracking progress against defined goals and establishing a process for ongoing reassessment of cryptographic security as quantum capabilities evolve**
• Identify PQC relevancy • Assign leadership and scope • Identify and engage stakeholders	• Establish or refine data inventory • Develop an inventory of cryptographic assets • Conduct risk assessment and determine urgency	• Select PQC algorithms and solutions • Prepare migration plan • Develop (internal) or acquire (external) solutions • Perform incremental roll-out	• Validate proper implementation • Track migration progress • Review and adapt • Train and prepare staff

Start with establishing an understanding of business processes – conduct a Business Impact Analysis (BIA)

- The goal of the BIA is to identify and evaluate potential disruptions to critical business operations due to unexpected events

- Use the BIA process to
  - Determine which business functions are **mission-critical**
  - Identify **dependencies** (people, processes, vendors, partners)
  - Identify critical **systems** and **applications**
  - Identify **data** required or produced

- Focus on identifying systems which
  - Process sensitive data with long confidentiality span
  - Support critical or long-lived infrastructure

Identify critical data processed or produced

Identify data

At rest: databases, repositories, disk encryption, etc.

In transit: TLS/SSL, VPN, secure protocols

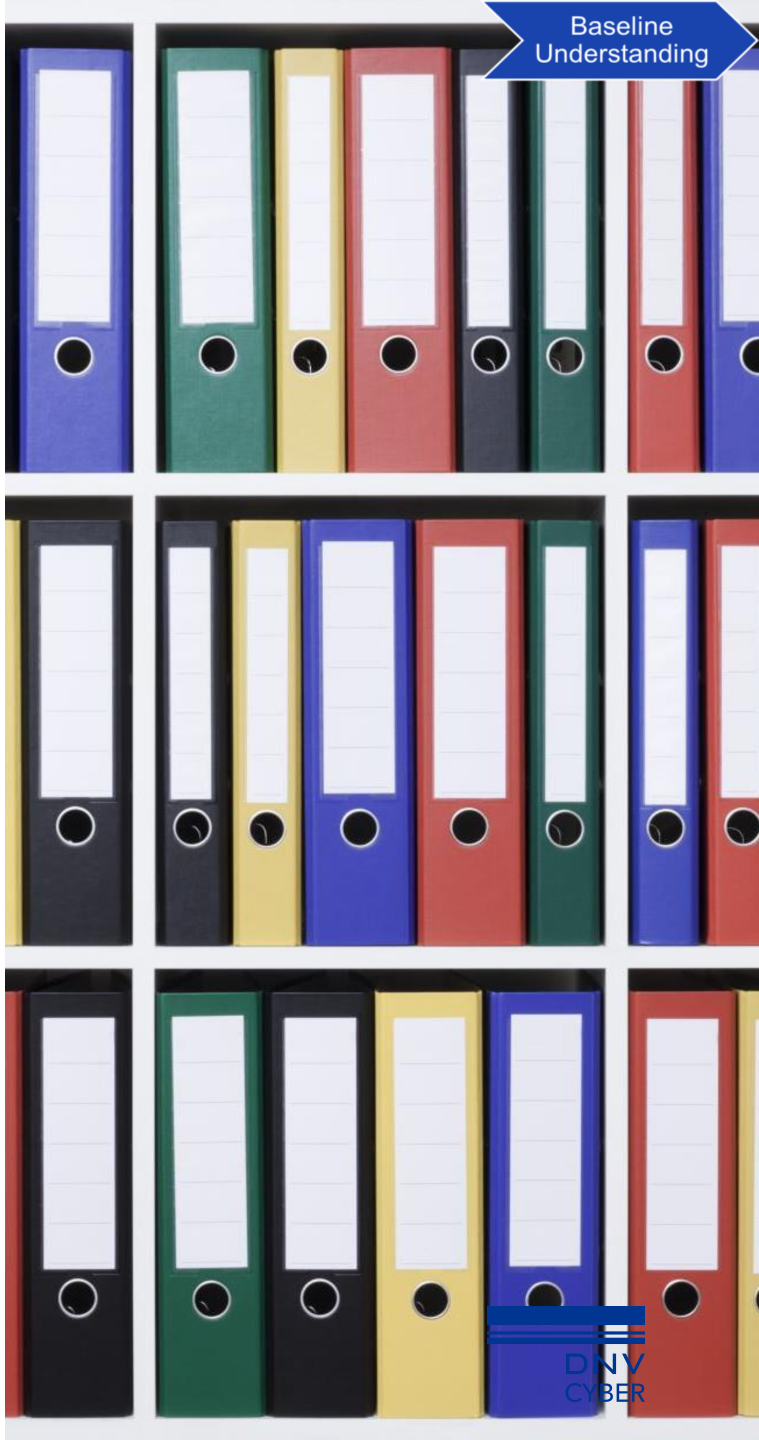
In use: secure enclaves, confidential computing

Focus on sensitive data with long confidentiality span

- Sources
  - Existing data inventories / asset registers
  - Business processes – BIA
  - Network topologies and data flows
  - Integration points / externally facing systems
  - Data repositories
  - Previous risk assessments

Build or refine a data inventory

- Collect and document critical data in an inventory
  - Data type
  - Where the data is stored, used, in transit
  - Information value
  - **Shelf-life** / lifespan, considering
    - Regulatory mandates
    - Auditing requirements
    - Intrinsic business value
  - Data **classification**
    - Protection needs
    - Regulatory or contractual obligations
  - Owner / responsible
  - Who has access to the data



Develop an inventory of cryptographic assets (next session)

- Identify and document cryptography in use
- Discovery exercises
  - How is data encrypted
  - Where are the keys managed
  - Who is responsible
- More details in next session

Baseline Understanding

Conduct quantum risk assessment to understand the cryptographic exposure and enable mitigation

- Assess the **potential impact of quantum computing** on systems, data, and business operations
  - Systems or data protected by cryptography that can be **broken** with a quantum computer
  - Sensitive data that can be **harvested** for “harvest now, decrypt later” scenarios

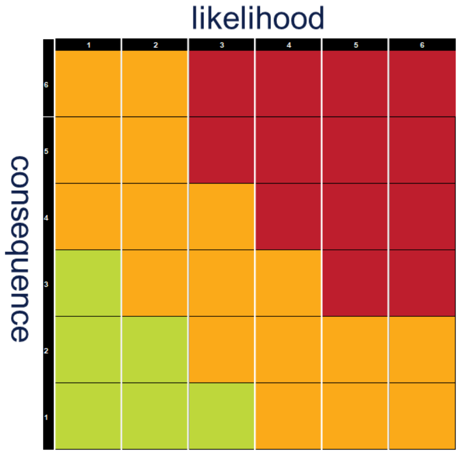
- NSM is recommending that we take into account that a potential threat actor is flexible and **has access to** cryptographically relevant quantum computers (CRQC)
  - A threat previously considered to be “benign” now becomes a major issue
  - Consider the consequence if your data is <u>already</u> exposed

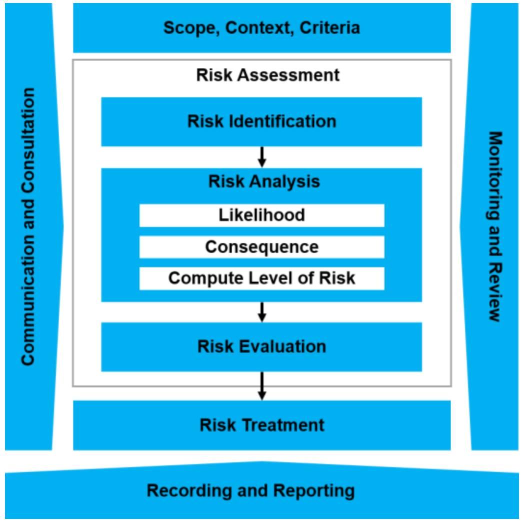
DNV CYBER

The purpose of cyber security risk assessment is to identify improvements to reduce risk

- Cyber risk = a **threat** exploiting a **vulnerability** in the digital environment, leading to adverse **consequences**

- A cyber risk assessment focuses on
  - Identifying **assets**/values, **threats**, and **vulnerabilities**
  - Assessing **consequences** in case of loss of confidentiality, integrity, or availability
  - Suggesting risk reducing **measures** through changes in technology, processes, or personnel capabilities




Scope, Context, Criteria

Risk Assessment

Risk Identification

Risk Analysis

Likelihood

Consequence

Compute Level of Risk

Risk Evaluation

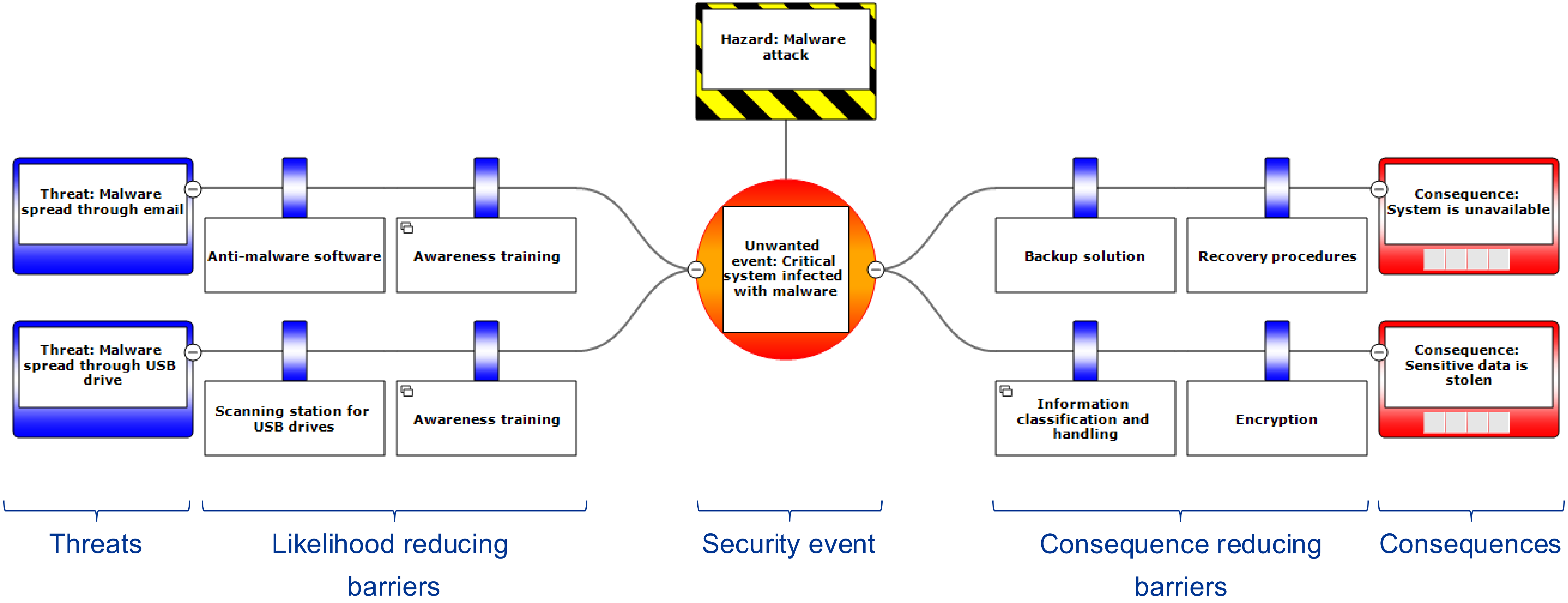
Risk Treatment

Communication and Consultation

Monitoring and Review

Recording and Reporting

A structured process for risk analysis is to use the bowtie model


Hazard: Malware attack
Threat: Malware spread through email
Anti-malware software
Awareness training
Threat: Malware spread through USB drive
Scanning station for USB drives
Awareness training
Unwanted event: Critical system infected with malware
Backup solution
Recovery procedures
Consequence: System is unavailable
Information classification and handling
Encryption
Consequence: Sensitive data is stolen
Threats
Likelihood reducing barriers
Security event
Consequence reducing barriers
Consequences

Baseline Understanding

Use historical data to identify relevant threats and attack scenarios

- A recommendation is to use MITRE ATT&CK® framework for identification of scenarios

THREATS

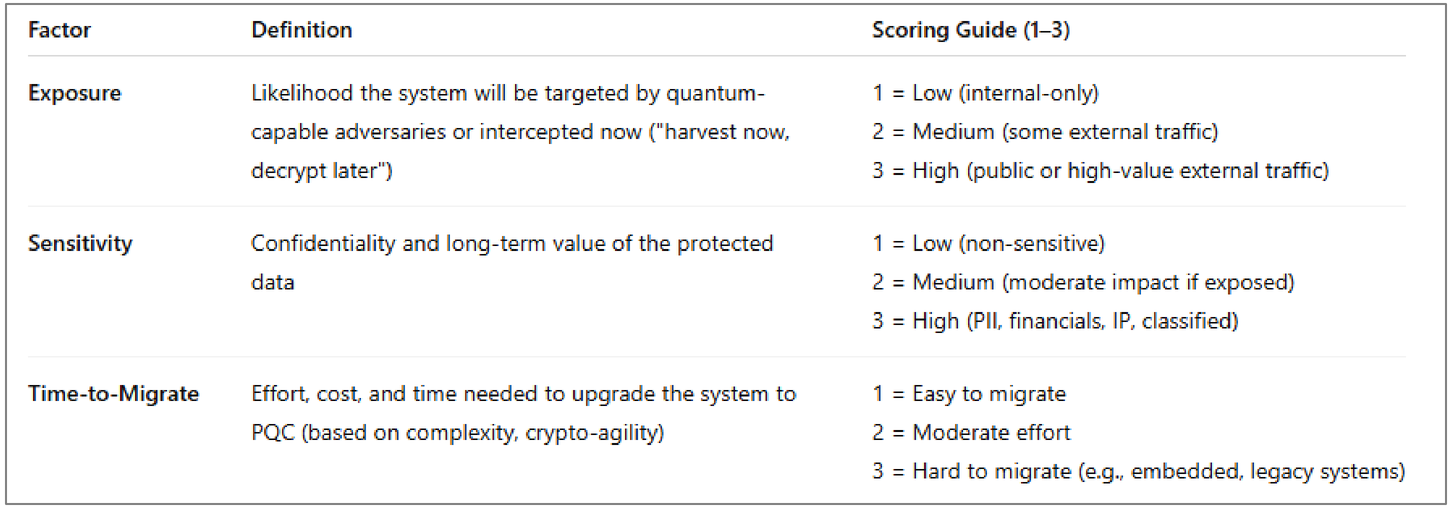
- Threat scenarios include:
  - Malware infection / Ransomware
  - Hacking
  - Denial-of-Service (DDoS)
  - Supply chain compromise
  - Malicious / negligent insiders
  - Social engineering
  - Unauthorized physical access

CONSEQUENCES

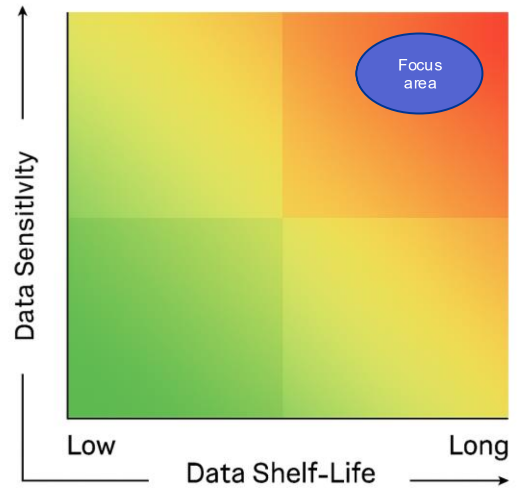
- System impacts include:
  - Data loss / theft
  - Data encrypted
  - Data manipulation / destruction / wipe
  - Service stop
- Business impacts include:
  - Operational disturbance
  - Financial loss
  - Brand damage / loss of confidence
  - Regulatory compliance / fines

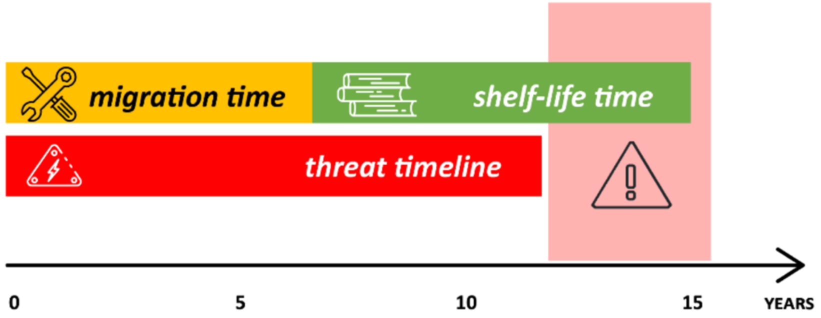
Use the data inventory and the risk assessment to determine urgency of PQC migration

- Focus on long-lived, high-value, externally exposed data
- Comply with any regulatory deprecation that mandates migration
- Use MITRE’s urgency scoring template
  - **Urgency Score = Exposure x Sensitivity x Time-to-Migrate**



Factor	Definition	Scoring Guide (1–3)
Exposure	Likelihood the system will be targeted by quantum-capable adversaries or intercepted now ("harvest now, decrypt later")	1 = Low (internal-only) 2 = Medium (some external traffic) 3 = High (public or high-value external traffic)
Sensitivity	Confidentiality and long-term value of the protected data	1 = Low (non-sensitive) 2 = Medium (moderate impact if exposed) 3 = High (PII, financials, IP, classified)
Time-to-Migrate	Effort, cost, and time needed to upgrade the system to PQC (based on complexity, crypto-agility)	1 = Easy to migrate 2 = Moderate effort 3 = Hard to migrate (e.g., embedded, legacy systems)





Group exercise

Group discussion – applying the framework to a financial institution

- **Scenario**: analyse a hypothetical financial institution with critical payment systems, customer data platforms, and long-term archival storage for regulatory compliance
- **Questions for discussion**:
  - Which business processes and systems are most critical to the financial institution's operations and rely heavily on cryptography?
  - What types of sensitive data handled by those processes have long lifespans (10+ years) and are therefore most vulnerable to "harvest now, decrypt later" attacks?
  - What would be the impact if encrypted data were harvested today and decrypted in the future?
  - Based on data sensitivity, longevity, and system criticality, what is the urgency level (e.g., immediate, near-term, long-term) for PQC migration for these identified assets? Justify the classification.
  - Who are the key internal stakeholders and external stakeholders that must be engaged in the Preparation phase to ensure alignment and resource allocation?

Thank you

Tor.Helge.Kristiansen@dnv.com

www.dnv.com/cyber

DNV
CYBER