

# The Future of Encryption:

Higher Education and Research  
Preparing for the Post-Quantum Shift

Craig Costello · AHECS Summit 2026



# RESEARCH DATA OUTLIVES SYSTEMS

## HARVEST NOW

Sensitive research shared today

## DECRYPT LATER

Confidentiality needed for decades

Confidentiality lifetime + migration time

# WHY Q-DAY COULD COME SOONER

Better Shor circuits

Less error-correction overhead

≈ 20×

fewer physical qubits

ECDLP-256 / secp256k1 estimate

Google Research, March 2026 · Resource estimate; Q-day remains uncertain

# WHAT BREAKS ON CAMPUS?

# TRUST

Federated identity

Research data links

Software & firmware



# PLAN NOW FOR 2030

**2026**

Refined plan

**2028**

Transition underway

**2030**

Transition complete

ASD recommended milestones, by year-end

# ONE RESEARCH WORKFLOW

## SIGN IN

University identity  
Federation + service



## MOVE DATA

Transfer endpoints  
TLS / SSH / gateways



## RUN ANALYSIS

Research cloud / HPC  
Libraries + signed code

At each boundary: what cryptography, whose change?

Illustrative workflow · confirm the actual protocols and owners

# PQC STANDARDS ARE READY

Deployment is  
the hard part



# CRYPTO AGILITY

Algorithms will change again

## CHANGE SAFELY

Keep research services running

Keys, certificates, protocols and hardware

PQC is the immediate test



# NO UNIVERSITY MIGRATES ALONE

Coordinate releases and testing



# PILOT ONE RESEARCH WORKFLOW

When can we test the full path?

Who owns each change?

A supported release, an owner and a test date

**CHOOSE A PATH**

**NAME ITS OWNER**

**BRING A PARTNER**

A funded pilot. A date to test together.