

PKI Under Pressure: The Executive Case for Modernization

A leadership brief for CIOs and CISOs
accountable for PKI resilience



PKI does far more than secure public websites. It establishes digital trust (identity, encryption, and integrity) for machines, software, and partner and supplier ecosystems.

When PKI works, it's invisible. When it fails, it leads to outages and customer impacts. PKI-related outages often occur because of an expired certificate. However, the cause is not the certificate. It's the failure to renew or deploy it in time.

These failures will become more frequent as pressure on PKI operations increases. For CISOs and CIOs, PKI modernization unlocks resilience, efficiency, and agility. A systematic approach reduces outages and lowers operational costs while enabling the business to safely adopt AI and stay secure against quantum threats.

A Quick Self-Assessment

A practical way for leaders to assess their PKI operations is to ask:



How many certificate-related outages and disruptions did we have in the last year?



Do we know about every PKI asset and which services it enables?



Do we consistently enforce policies and assign ownership across our enterprise, clouds, and third-party ecosystems?



Can we renew, install, or revoke certificates without delays or heroics?

The answers, or lack thereof, indicate if PKI is being managed as a strategic capability or as a set of disparate tasks across siloed teams.

The 2026 Global PKI Research Report shows that IT and security decision-makers understand that incomplete visibility into PKI contributes to continued outages.

34% have a complete, up-to-date certificate inventory

73% are very or extremely concerned about outages

74% are concerned about certificate sprawl

Set Targets to Begin Modernization

Inventory is the first practical step, but the broader goal of PKI modernization needs to be a funded and accountable priority.

That starts with three commitments:

1. Set an outage-reduction target

The practical benefit of modernization is fewer outages and near misses. Set an outage-reduction target as your north star.

2. Find your centers of excellence

One or more teams in your enterprise are on their way or have achieved PKI modernization. Find those teams and use them as the mold for your other instances of PKI.

3. Know your limits

From architecture to operations, PKI requires specialized skills. You will need to apply these skills to your own infrastructure and where it intersects with third-party systems. Expect to advise your partners and suppliers. Expect to train your existing staff and augment them when needed.

These commitments begin to give PKI modernization the top-level guidance and sponsorship it needs so your team can be successful.



52%

Expect PKI investments
to increase

68%

Are actively modernizing or
plan to in the next 1-2 years

60%

Report reduced outages
as one of the outcomes

digicert® ONE

DigiCert ONE unifies certificate lifecycle management, PKI, and DNS under a single governance and automation layer.

It empowers organizations to replace fragmented tools and siloed PKI environments with one scalable platform.

To learn more about the return on investment of DigiCert ONE, read [The Business Case for Modernization](#).

Read the complete [2026 Global PKI Research Report](#).

