digicert®

Certificate Management at 47-day Speed

Key findings from DigiCert's Certificate Management Outlook

Research Report | 2026

Certificate management is entering a new operating era

The era of manual certificate management is coming to an end as the industry moves toward 47-day public TLS certificates. Enterprises will need to renew certificates more than eight times as often as they do today and perform 40 times as many domain validations. At that scale, spreadsheets, manual processes, and fragmented tools simply weren't designed for that pace.

Almost three-quarters of IT and security leaders expect certificate volumes to increase over the next two years, as CA/Browser Forum changes dramatically increase the frequency of certificate renewals and domain validations. This leaves organizations with more certificates to manage across shorter lifecycles. Greater visibility and automation will be essential to handling that scale without increasing operational risk or disruption.

The impact of certificate failure already extends beyond the security team. When a certificate causes an outage, 57% of organizations categorize it as an IT infrastructure issue, compared with just 17% that categorize it as a security incident. For customers, that makes effective certificate management an infrastructure resilience issue, not simply a PKI concern.

The financial stakes are rising as well, with nearly one in four organizations reporting that the financial impact of their most significant certificate incident cost more than $250,000, up 18% compared to a year ago. More than a third also experienced a service outage caused by an expired certificate, underscoring the business impact when certificate lifecycles are effectively managed. Against that backdrop, automated certificate lifecycle management now ranks as the third-highest cybersecurity priority among those surveyed.

Discover how 1,001 IT and security leaders are managing certificate risk, preparing for shorter lifespans, and adapting certificate management for the 47-day era.

The rising cost of certificate failures

Key findings

34% experienced certificate expiration leading to a service outage.

40% experienced service downtime due to certificate mismanagement.

23% said their most significant certificate incident cost more than $250,000, up from 18.5% a year ago.

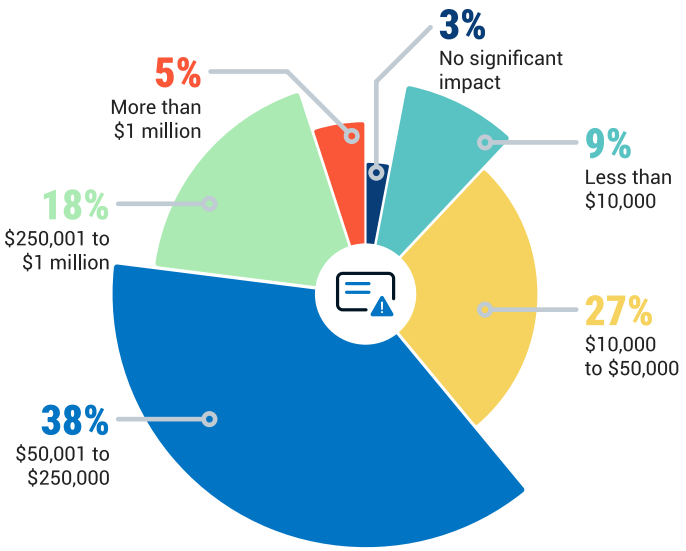
Nearly three quarters of organizations experienced at least five hours of downtime caused by certificate issues over the past year, while 21% experienced 25 hours or more. Expiration remains a common cause of outages, leaving organizations exposed when certificate tracking and renewal depend on manual processes.

The financial impact is also becoming more severe. The share of organizations reporting incidents above $250,000 has risen by 4.5 percentage points in just one year, even as outages caused specifically by expired certificates have remained relatively stable. The frequency of the problem may not be increasing, but the cost when things go wrong is.

57% categorize certificate outages as IT infrastructure issues, compared with 17% that categorize them as security incidents.

How organizations record these outages shows how far that impact can reach, making certificate management an operational resilience concern rather than one confined to PKI or security teams.

What was the financial impact of organizations' most significant certificate incident?



Manual certificate management won't scale

Key findings

56% manage more than 1,000 digital certificates.

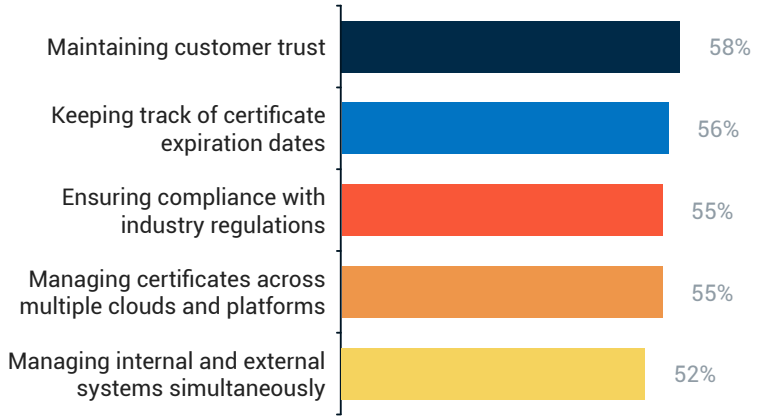
49% work on certificate management and related security tasks 12+ times per year.

56% are very or extremely concerned about certificate expiration.

Certificate volumes already run into the thousands for more than half of organizations surveyed. The work is recurring, with another 39% of IT teams handling certificate management and related security tasks between six and 10 times per year.

When issuance, renewal, deployment, and remediation require manual intervention, that scale creates a steady demand for IT resources. Expiration remains a persistent concern at broadly the same level as last year, while teams are also contending with compliance, customer trust, and certificates spread across multiple platforms and environments.

What certificate management challenges were listed as a combination of very or extremely concerned?



47 days raises the bar for certificate management

Key findings

72%
expect certificate volumes to increase over the next two years.

70%
are actively preparing for shorter certificate lifespans.

22%
know about the changes but have not started preparing.

With 14% expecting certificate volumes to grow by more than 30%, organizations face larger certificate estates and increasingly compressed lifecycles. They aren't simply preparing for more frequent renewals; they will need to discover, validate, issue, and deploy certificates at a much faster pace across growing environments. The organizations best prepared for 47 days won't simply automate renewal; they'll automate the certificate lifecycle.

Preparation varies by market: 74% of U.S. organizations are actively preparing, followed by 71% in the U.K. and 62% in Australia—a 12-percentage-point gap between the most and least prepared markets. For organizations still relying on manual processes, that faster lifecycle makes automation increasingly important to maintaining security without adding operational risk.

Why are certificate lifespans shrinking?

The CA/Browser Forum adopted the phased reduction to strengthen Web PKI security. Shorter lifespans mean certificates and validation information are refreshed more often, reducing the amount of time outdated or potentially compromised credentials remain valid. More frequent renewal improves security, but it also puts certificate management on a much faster cycle.

Automation is becoming a cybersecurity imperative

Key findings

46% prioritize automated certificate lifecycle management, making it the third highest cybersecurity priority.

Over the next **12 months**, DevOps integration ranks first among certificate management improvement priorities.

44% experienced compliance challenges related to certificate management in the past year.

At 46%, automated certificate lifecycle management ranks behind only security operations powered by AI at 65% and software threat detection and response at 61%. Certificate management has moved well beyond a specialist PKI concern and onto the broader CISO agenda.

The priorities for the next 12 months also extend beyond renewal. Visibility, compliance, software supply chain security, and reducing manual effort all rank ahead of automated certificate renewal. The message is clear: certificate automation can't stop at renewal. It needs to extend across the lifecycle and into the systems, teams, and workflows where certificates are used.

Priorities vary by market. Expanding compliance programs ranks first in Australia, while improving certificate visibility leads in both the U.S. and U.K.

Make certificate investment deliver more

Key findings

53%

allocate more than 10% of their security budgets to certificate management and related solutions.

29%

point to executive buy-in or an unclear ROI or business case as their biggest automation barrier.

25%

Legacy system incompatibility is the leading barrier to automation, at 25%.

Organizations are already committing meaningful security budget to certificate management, yet budget remains the second most common barrier to further automation at 21%. For security leaders, that puts more emphasis on showing what the investment returns to the business, from fewer outages and less manual work to stronger operational resilience.

Skills are another constraint, with 14% pointing to a lack of technical expertise. When asked about barriers to implementation, just 10% selected “already have automation in place." Moving forward will require organizations to make automation work across existing environments while building the internal case to fund it.

Making the business case

A DigiCert-commissioned Forrester Total Economic Impact™ study of DigiCert ONE found that a composite organization achieved 312% ROI over three years, with payback in less than six months. In addition, automation eliminated more than 160,000 hours of manual certificate work.

The findings help quantify the business case for automation by showing how reduced manual effort can translate into greater operational efficiency and measurable financial returns.

Explore the Total Economic Impact™ of DigiCert ONE

The path forward: Automation strengthens business resilience

Certificate outages rarely stop at the certificate itself. Most organizations categorize them as infrastructure issues rather than security incidents, reflecting how deeply certificates are embedded across applications, services, and the wider technology environment. When they fail, the impact can reach critical services, productivity, revenue, customer experience, and reputation.

Enterprises are already absorbing significant downtime and rising financial costs from certificate incidents, while maintaining customer trust remains their leading certificate management concern. As certificate volumes grow and lifecycles shorten to 47 days, relying on manual processes to manage that exposure will become increasingly difficult.

The shift to 47-day TLS isn't simply a certificate-renewal challenge. It's a forcing function for how enterprises discover, govern, automate, and manage trust across their infrastructure.

Addressing that shift requires greater visibility, control, and automation across the certificate lifecycle, reducing manual intervention and the risk of avoidable outages. For security leaders, the opportunity is bigger than operational efficiency: it is to lower costs and risk while building greater resilience and interoperability into the digital infrastructure the business depends on.

Prepare for shorter certificate lifecycles with DigiCert

DigiCert Trust Lifecycle Manager gives you the visibility, governance, and automation to manage public and private certificates at scale, preventing avoidable outages and keeping pace as certificate lifecycles shrink.

[Find out more]

Methodology

This report is based on findings from an independent survey conducted by Propeller Insights on behalf of DigiCert in May 2026. The study surveyed 1,001 IT and cybersecurity decision-makers across three markets: the United States (500 respondents), the United Kingdom (251 respondents), and Australia (250 respondents).

Respondents represented organizations across a range of industries and company sizes and included professionals responsible for cybersecurity, IT infrastructure, risk management, compliance, digital transformation, and technology strategy. The survey explored organizational readiness and investment priorities related to artificial intelligence (AI), machine identity security, governance, cryptographic resilience, certificate lifecycle management, and emerging cybersecurity risks.

Data was collected through an online survey and analyzed in aggregate to identify trends, priorities, challenges, and opportunities shaping the future of intelligent trust. Percentages reported throughout this report may not total 100% due to rounding.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management to secure infrastructure, software, devices, messages, and AI content, agents, and models. Learn why more than 125,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com