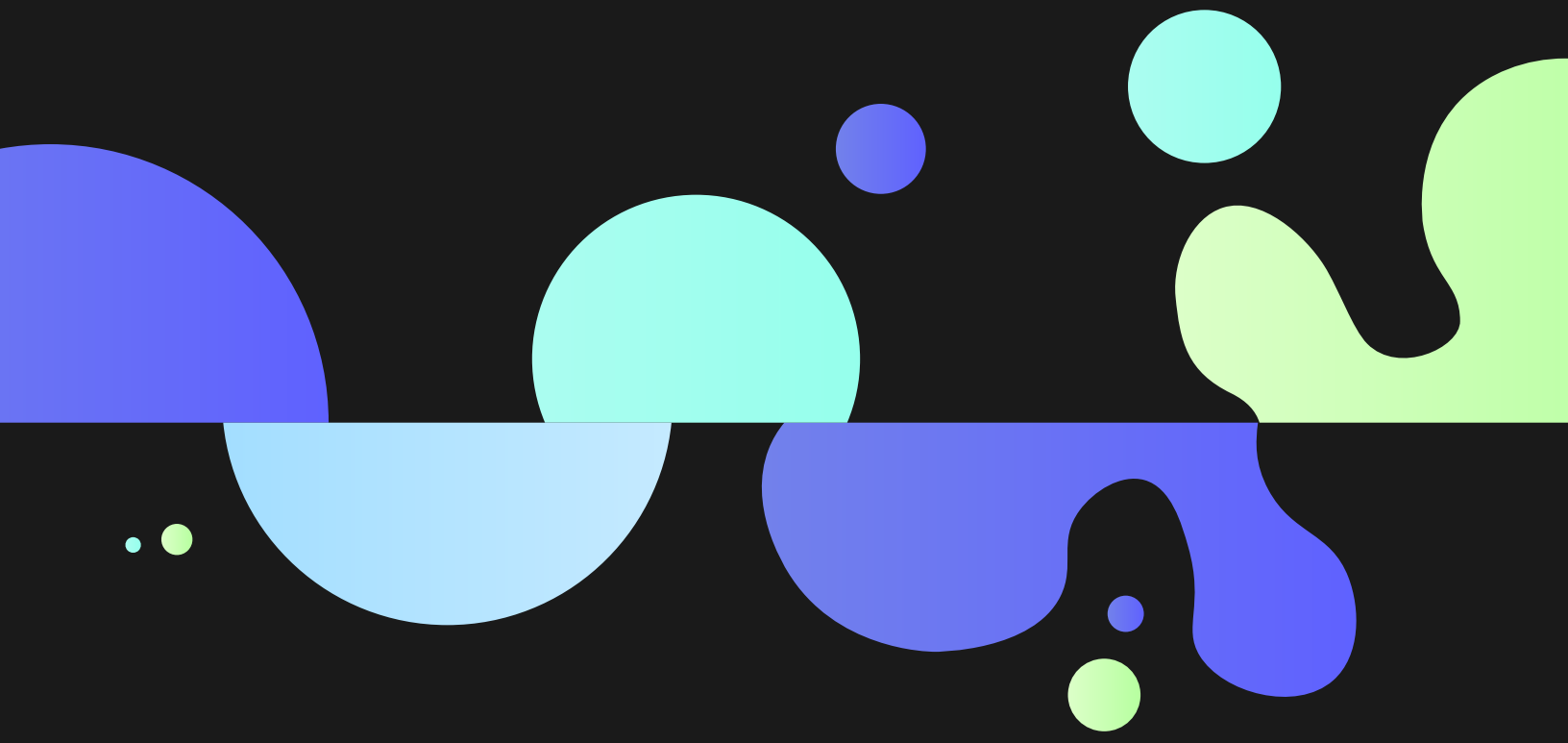
KEYFACTOR

VansonBourne

Global report

2024 PKI & Digital Trust Report



Executive Summary

In an era defined by digital transformation, building strong digital trust has become paramount. The World Economic Forum (WEF)[1] identifies three concepts that, when combined, create an environment of digital trust. This includes security and reliability, accountability and oversight, and inclusive, ethical, and responsible use. Organizations are responsible for establishing and maintaining their own digital trust, with identity management at the center.

The use of digital certificates has grown exponentially, and organizations have looked to harness the power of PKI to authenticate humans and machines, encrypt sensitive data, and enable secure communications.

The sheer volume of certificates to manage has, in many cases, overwhelmed IT teams with operational inefficiencies, security vulnerabilities, and compliance risks; inevitably shaking digital trust. Preserving and building digital trust is essential to foster confidence in the reliability and security of organizations' PKI, as well as supporting innovative new products and business opportunities.

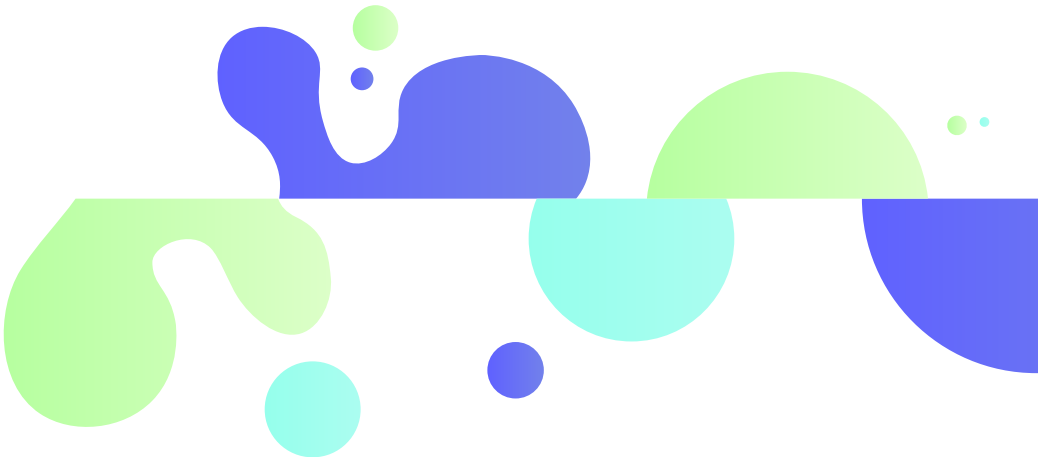
Simultaneously, the advancement of quantum computing signals a new era of technological advancement. The potential of quantum computing to undermine widely used security protocols and algorithms is clear, with the threats to encryption and other security measures of high concern; and it should be. The state of digital trust hangs in the balance as quantum computing rapidly develops, and organizations need to prepare. The journey to post-quantum cryptography (PQC) is widely spoken about, but organizations have many challenges to overcome before they can be prepared.

This report delves into the state of PKI and digital trust, exploring the complexities of managing PKI and digital certificates, and organizations' journeys toward PQC readiness. In identifying and navigating these key areas, organizations can look to traverse the complexities of digital trust with confidence, ensuring the effectiveness and relevance of PKI in a rapidly evolving digital landscape.

Chris Hickman,
Chief Security Officer, Keyfactor

[1] - https://initiatives.weforum.org/digital-trust/framework

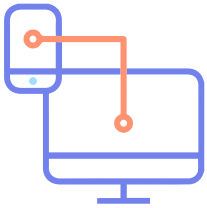
Contents



Key definitions

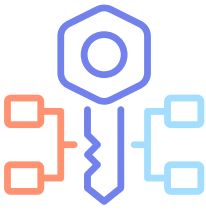
Machine identities:

Machine identities are unique descriptors of an organization's devices used for system access and to authenticate and encrypt communications. Essentially, they are digital credentials that identify servers, computers, phones, and other Internet of Things (IoT) devices.



Machine identity management:

As machines (either hardware or software) interact with other entities such as devices, applications, cloud services, or gateways, these connections must be secure and trustworthy. Machine identity management provides centralized visibility, control, and management of the endpoints and their supporting infrastructure.

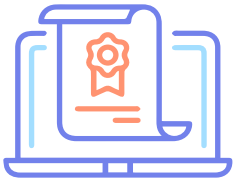


PKI:

Public key infrastructure (PKI) governs the issuance of digital certificates to protect sensitive data, provide unique digital identities for users, devices, and applications, and secure end-to-end communications.

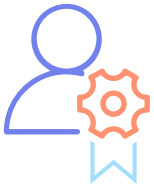
Certificate Authority:

The Certificate Authority (CA) is a trusted source that issues digital certificates and manages their life cycle, including generation, revocation, expiry, and updating. They are responsible for attesting to the identity of users, computers, and organizations, and authenticating an entity, vouching for that identity by issuing a digitally signed certificate.



Digital certificates:

Digital certificates are the primary vehicle by which people and machines are identified and authenticated. A digital certificate is a file or electronic password that proves the authenticity of a device, server, or user through cryptography and the public key infrastructure (PKI). Digital certificate authentication helps organizations ensure that only trusted devices and users can connect to their networks.



Certificate Management:

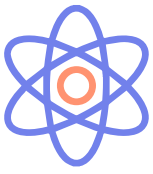
Certificate Management involves discovering, analyzing, monitoring, and managing all digital certificates deployed by the Certificate Authority (CA).

Keys:

A key is something that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (the private key).

Cryptography:

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and e-commerce.



PQC:

Post-quantum cryptography (PQC) is the development of cryptographic algorithms (usually public-key algorithms) that are thought to be secure against an attack by a quantum computer.

Key Findings

99.8% respondents reported that their organization has a machine identity strategy in place, with over half (55%) believing their strategy to be fully mature

Despite this, the majority of organizations (93%) are experiencing challenges with setting their strategy, and 72% agree that machine identity management is problematic to their organization

Looking to 2024 and beyond, organizations have identified the top trends driving the deployment of PKI, keys, certificates and other secrets;

48% Increasing use of BYO mobile devices

46% Increasing use of AI/Generative AI

46% Internet of Things devices within organizations

81% agree that misconfiguration of PKI and certificates is an increasing concern; and this concern is only increasing, up from **55% in 2021 to 58% in 2023**

It's clear that PKI is critical infrastructure, supporting business-critical applications like web servers (41%), product security (40%) and Wi-Fi and network equipment (39%), yet only 2% of organizations are confident in their current approach. Nearly all (98%) organizations would make changes to their PKI across many areas, including relevant security stakeholders for tackling compliance and governance requirements (49%), better preparing for scaling and organizational growth (48%), and adding more automation (40%)

Certificate sprawl is evident

91%

of respondents agreeing their organization is deploying greater volumes of cryptographic keys and digital certificates

84% agree that the growing use of cryptographic keys and digital certificates is significantly increasing the operational burden on teams, but only 32% of organizations are using dedicated certificate lifecycle management software to track and manage their certificates

When issues arise with certificates, it's often due to a lack of management, which can create substantial negative impacts on a business. For example, with certificate outages caused by expired certificates:

48% report customer confidence would likely be affected

46% report that brand reputation would be impacted

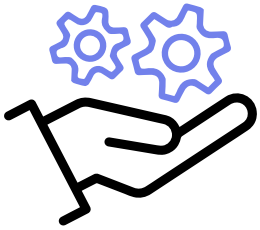
37% report revenue loss

To achieve their strategic aims for effective PKI management and maintenance, organizations are aware that they need to invest both...

...in their staff...

71%

...and resources

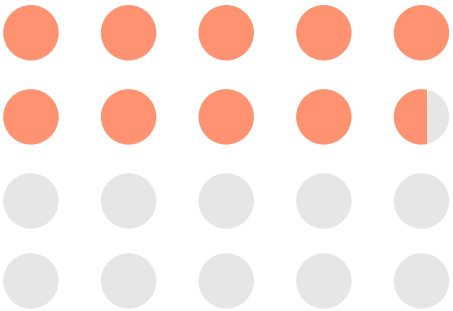


75%

In the past 24 months, organizations reported 3 incidents on average occurring in each of the following areas; certificate outages or expiration, failed audits and security breaches or incidents. These take nearly 3 hours to identify, and another almost 3 hours to remediate, with 8 staff directly involved in these processes, on average.

48%

Navigating the increasing use of AI-powered systems and AI-generated content is the top machine identity management strategy priority for 2024



Organizations are also cognizant of the advancements in quantum computing and its impact on cryptography - 23% reported that their post-quantum cryptography (PQC) planning is a work in progress, while 36% are expected to start this year after the first release of standards (2024)

Challenges remain, however, with 95% reporting their organization is encountering obstacles in the process of getting ready for PQC

Strategic priorities for machine identity management

With an ever-increasing number of devices, applications, and services being used by organizations, non-human entities (or machines) must be authenticated and verified with a trusted identity; this is where machine identity management comes in, with centralized visibility, control, and management of the machine identities and their supporting infrastructure. The notion that machine identity management is critical to successful security is something that organizations are well-accustomed to, with PKI serving as the backbone for establishing and maintaining digital trust in modern computing environments.

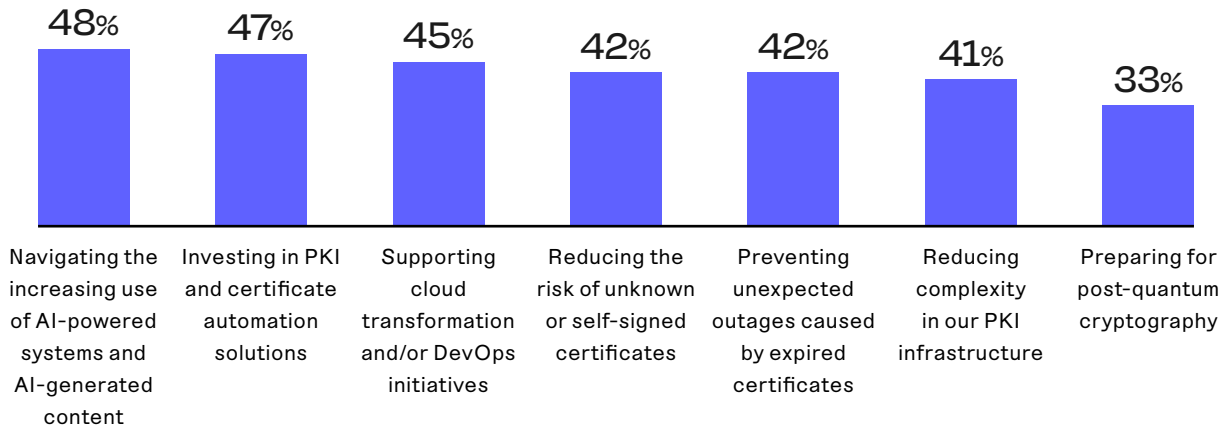
Therefore, it's no surprise that nearly all (99.8%) respondents report that their organization has a strategy in place. Over half (55%) say that their strategy is fully mature, consistently applied across all their applications and use cases. While organizations may believe that their machine identity management strategies are fully mature, often issues surrounding comprehensive visibility or managing certificates at scale are experienced, which we explore throughout this report.

To address challenges and enhance their machine identity management, organizations are prioritizing several strategic initiatives in 2024.

Figure 1:

Strategic priorities for machine identity management

What are your strategic priorities for machine identity management within your organization? [1200] Not showing all answer options.



Navigating and leveraging the increasing use of artificial intelligence (AI) systems and generated content (48%) is among the most common priorities. AI-powered applications are driving an increase in machines and servers to support them, creating the need for more machine identities, and therefore likely additional management from organizations and support from vendors.

In addition, it is imperative to trust the integrity and authenticity of AI content, making it essential that AI-generated images and videos are digitally signed. Initiatives, such as the Coalition for Content Provenance and Authenticity (C2PA[2]), aim to address the prevalence of misleading information online and is essential to trusting digital content.

> ***Initiatives, such as the Coalition for Content Provenance and Authenticity (C2PA), of which Keyfactor is a member, play an important role in ensuring we can trust the integrity and authenticity of the content we consume***
>
> Chris Hickman, Chief Security Officer at Keyfactor

[2] - https://c2pa.org/

The second-most priority for strategy is investing in PKI and certificate automation (47%). PKI and certificates are highly integrated into almost all departments and teams, from IT and security to platform engineering and cloud teams. It is, therefore, paramount that organizations manage and govern their PKI effectively, and a key part of this is automation. Ensuring that it is usable and scalable for all teams that depend on PKI and certificate usage is pivotal in streamlining processes, reducing manual errors, and enhancing operational efficiency.

The third priority for machine identity management strategy is to support cloud transformation and/or DevOps initiatives (45%). For organizations that are looking to scale and automate their machine identities, keys, and certificates, this will play an essential role in securing these fast-moving environments. By allowing rapid deployment and scalable applications and services, organizations can ensure the robust protection of their digital assets while enabling rapid innovation and growth.

With only a third (33%) reporting they are preparing for PQC as a strategic priority, this is a promising start in the long journey ahead to post-quantum readiness. However, the challenges ahead are significant, and organizations need to prepare for it, as we discuss later in section 5.

PKI and certificate usage

Organizations are using PKI and certificates for various applications, with many using them for vital services such as their web servers, product security, and Wi-Fi and network equipment.

Figure 2:
What is your organization currently using PKI and certificates for? [1200] Not showing all answer options.

41%
Web Servers (SSL/TLS)

40%
Product Security

39%
Wi-Fi and Network Equipment

While AI was indicated as a top strategic priority, only 4 in 10 (37%) organizations currently use PKI to support AI and AI-generated content, suggesting that most teams are in the early stages of navigating security in this arena. Many (91%) also agree that PKI is one of the most important solutions to protect their organization against threats posed by AI. Ensuring that AI is adopted in a way that preserves trust and security is vital, and organizations must implement AI in a way that protects their underlying infrastructure and services — as well as any content or code produced from AI-generated sources.

Figure 3:
To what extent do you agree or disagree with the following statements? - PKI is one of the most important solutions to protect my organization against threats posed by AI [1200] Showing the combination of those that strongly agree and agree.

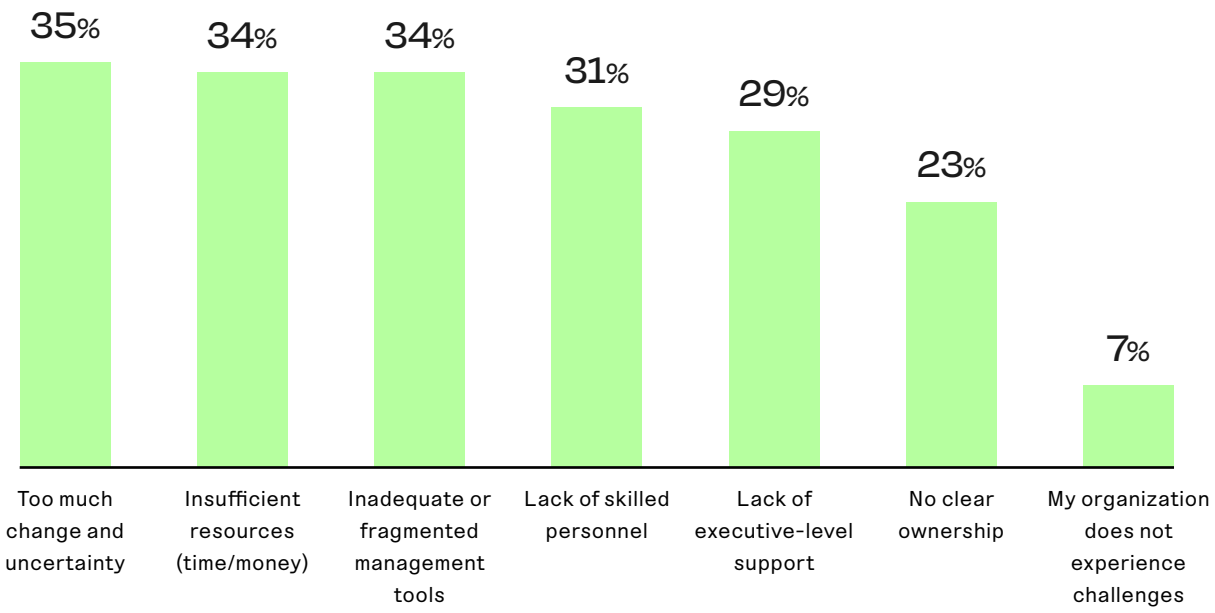
Challenges faced in PKI and machine identity management

Despite self-reported maturity (page 9) and the importance of having a clear and defined PKI and machine identity management strategy, the majority of organizations (93%) are experiencing challenges when it comes to implementation.

Figure 4:

Challenges involved in setting an enterprise-wide PKI and machine identity management strategy

What are the main challenges involved in setting an enterprise-wide PKI and machine identity management strategy in your organization? Asked to respondents whose organizations have a strategy for machine identity management. [1198] Not showing all answer options.



In 2024, the greatest challenge lies around high levels of change and uncertainty, which is unsurprising when considering the economic turbulence and geopolitical landscape over the last few years. Similarly, regulatory uncertainty and concerns over compliance gaps, evolving standards, and legal risks mean organizations have many areas to monitor and react to.

This, in many cases, can also lead to budgetary and time constraints, with over a third being challenged by insufficient resources, such as time or money. Organizations are having to fight harder than ever to be able to prioritize their PKI and machine identity strategy. This is made more difficult given the specialized nature and the specific skill set required to manage PKI, meaning that it is not always easy to find or train the talent required.

Organizations are also encountering inadequate or fragmented management tools. With this increasing year on year, from 23% in 2021, to over a third in 2024 (34%), it demonstrates that PKI and certificate sprawl are a real and growing problem, where legacy tools cannot keep up. With so many different tools available to use, different teams are likely using the tools they prefer, creating an untenable situation. Decentralized PKI is the new reality for many[3], but organizations must work to simplify, consolidate, and govern their PKI infrastructure and certificates across the business.

Despite these challenges, organizations must address these issues proactively to establish a secure and resilient PKI infrastructure and machine identity management framework. By investing in expertise, as well as leveraging scalable, consolidated, and integrated solutions, organizations can look to overcome these challenges and mitigate security risks effectively.

[3] - https://www.keyfactor.com/blog/decentralized-pki-the-new-reality

Outages, failed audits, and security incidents

Inadequate tools and resources inevitably lead to gaps in visibility and protection, which, in the case of PKI and certificate management, often results in outages, compliance issues, and security incidents.

Over the past two years, organizations have experienced an average of 9 machine identity-related incidents, including outages caused by expired certificates, unenforced or insufficient keys or policies, and lost or stolen keys or certificates. While organizations report maturity in their machine identity management strategies (page 9), challenges and real-life experiences suggest otherwise; there is a disconnect between perception and reality.

In section 4, we later explore the cost of these experiences and why organizations must carefully consider how to best manage their strategy and solutions used to reduce risk and further establish maturity.

Figure 5:
Approximately, how many times has your organization experienced the following during the past 24 months? [1200]
Showing the average number of times.

3
incidents on average, where an **outage** in which an **expired certificate** was the **root cause**

3
incidents on average, where a **failed audit** or **lack of compliance** from **unenforced/insufficient key** or certificate management **policies**

3
incidents on average, where a **breach** or **security-related incident** due to **lost or stolen keys or certificates**

Certificate volume growth

Despite the fact that organizations report they have a mature machine identity management strategy, they also admit that they are struggling when it comes to implementation and when things do not go to plan. The reality is clear; many are struggling with machine identity management.

Figure 6:
To what extent do you agree or disagree with the following statements? - Machine identity management is problematic in my organization [1200] Showing the combination of those that strongly agree and agree.

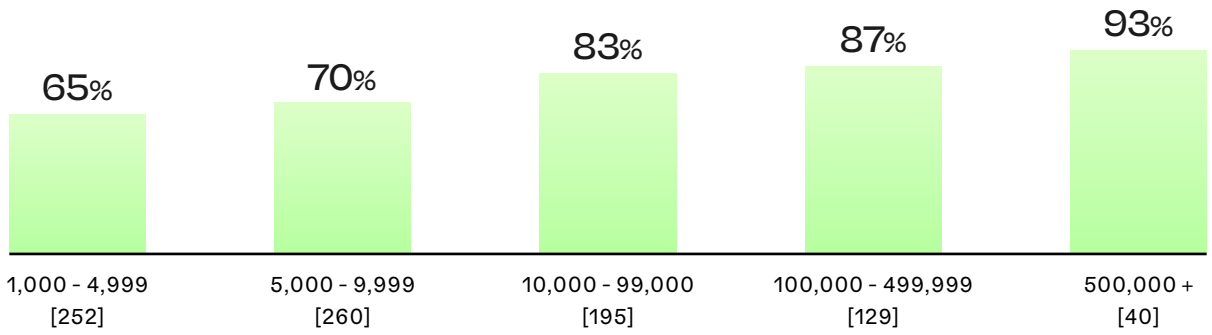
72% agree that machine identity management is problematic in their organization

The more certificates that organizations have, the more problems they experience. Organizations experiencing growth are likely to see an increase in the volume of certificates they must manage, and they are finding this increase unmanageable.

Figure 7:

Those that agree machine identity management is problematic in their organization, by the number of internally trusted certificates they have

To what extent do you agree or disagree with the following statements? - Machine identity management is problematic in my organization [base numbers in chart] Showing the combination of those that strongly agree and agree, split by the number of internally trusted certificates that they have in their organization.



Further to the worries with certificate volume growth, a high majority agree that misconfiguration of PKI and certificates is an increasing concern; rising year-over-year from 55% in 2021 and 2022, to 58% in 2023. Misconfiguration can have severe implications for security, compliance, and operational efficiency, which is clearly something that organizations need to avoid. As time and concern increase, it's clear that organizations have not yet got a handle on their PKI and certificate management and automation.

Figure 8:

To what extent do you agree or disagree with the following statements? - Misconfiguration of PKI and certificates is an increasing concern in my organization [1200] Showing the combination of those that strongly agree and agree.

81% agree that misconfiguration of PKI and certificates is an increasing concern

Public Key Infrastructure (PKI)

Achieving strategic aims in PKI

As organizations look to continue their evolution and adapt to emerging threats and technological advancements, the strategic importance of PKI becomes increasingly apparent. With the growing number of certificates and challenges experienced, it's no surprise that most report that more staff and resources are needed to manage and maintain their PKI.

Building and maintaining a robust PKI infrastructure requires a skilled workforce with high levels of expertise, and currently, a large number of organizations believe that they need more staff to manage and maintain their PKI. Attracting those with experience in this area can prove difficult; therefore, investing in staff development programs, training initiatives, and certifications to enhance the knowledge and skills of their current cybersecurity staff is a practical route to support PKI and organizational growth.

Beyond increasing and upskilling staff, effective PKI implementation and management requires adequate resources – such as funding, infrastructure, and technology investments. Organizations can achieve their strategic aims in PKI by allocating resources and intentionally prioritizing investments in critical areas such as cryptographic hardware, certificate management platforms, and security controls. With three-quarters feeling that more resources are required to manage and maintain their PKI, organizations need to align their resource allocation with their business objectives alongside regulatory compliance. This will enable their successes to be optimized and ensure the resilience, scalability, and effectiveness of their PKI infrastructure.

Figure 9:
In your opinion, does your organization have enough resources and staff to manage and maintain PKI effectively? [1200] Showing the combination of those that state their organization needs considerably more or slightly more to manage and maintain their PKI.

71%

report that their organization needs more **staff** to manage and maintain their PKI

75%

report that their organization needs more **resources** to manage and maintain their PKI

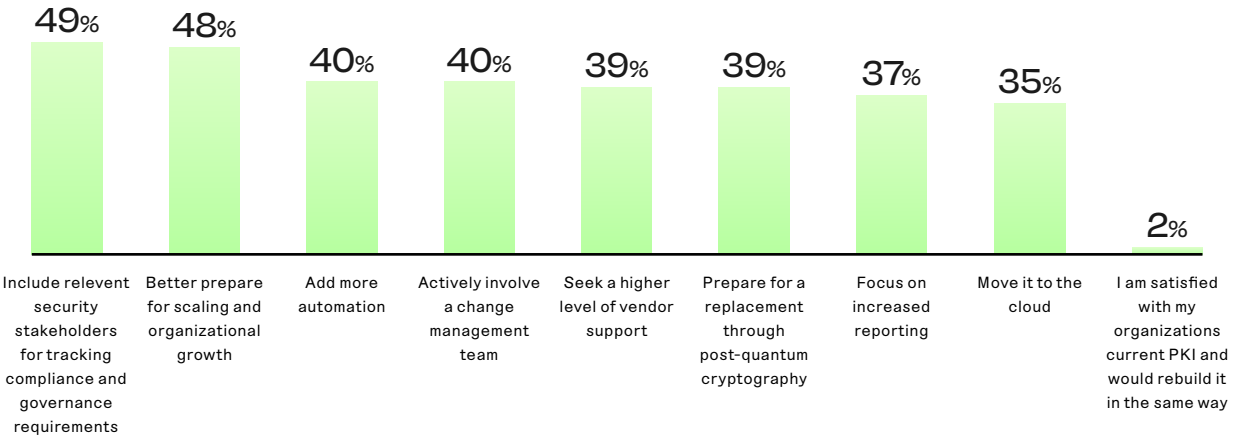
The changes organizations would make to their PKI

If given the opportunity, nearly all (98%) respondents say they would change their organization's PKI. And can you blame them? With so many grappling with a growing number of certificates and a range of challenges and limitations with their existing PKI, there is much to do to improve their current tools, infrastructure, and processes.

Figure 10:

What organizations would do if they could re-build their PKI today...

If I could re-build my organization's PKI today, I would: [1200] Not showing all answer options.



Only 2% of respondents are satisfied with their current PKI, stating that they would rebuild it similarly, so it's clear that the current PKI setup is inadequate for the vast majority. Changes are across many areas, such as including relevant security stakeholders for tracking compliance and governance requirements (49%), better preparing for scaling and organizational growth (48%) and adding more automation (40%). Stakeholders must balance the need for speed and scale with the need for security and best practices, and these changes should address their evolving business needs, technology advancements, and security threats.

It's unsurprising to see that, if organizations could re-build their PKI today, 39% would prepare to replace their PKI to support post-quantum cryptography. As quantum computers develop and new quantum-resilient standards near production-ready use, it's clear that organizations will need to make significant changes in the coming years. The introduction of quantum-resilient algorithms will create new challenges for compatibility, performance, and scale, and navigating these challenges will take years, highlighting the need to start planning and testing today.

The increasing volume of certificates and issuing Certificate Authorities (CAs)

Certificate lifecycle management is becoming increasingly challenging as the number of digital certificates continues to rise each year. With the proliferation of digital services, IoT devices, cloud workloads, and AI capabilities, organizations face the daunting task of managing a growing number of keys and certificates.

Figure 11:
To what extent do you agree or disagree with the following statements? - My organization is deploying more cryptographic keys and digital certificates [1200] Showing the combination of those that strongly agree and agree.

91% agree their organization is deploying more cryptographic keys and digital certificates

A high majority (91%) of organizations report that they are deploying more cryptographic keys and digital certificates than ever before, and this is growing every year. This was reported by 61% in 2021 and 74% in 2023, demonstrating an increasing trend, creating a feeling that teams responsible for PKI are struggling to maintain this increasing volume.

Figure 12:
Approximately, how many internally trusted certificates would you estimate your organization has (e.g., certificates issued from an internal private Certificate Authority [CA])? [1200] Showing average number of certificates used. Approximately, how many different internal issuing Certificate Authority's (CAs)/ Intermediate Certificate Authority's (ICAs) do you estimate are in use across your organization? [1200] Showing average number of CAs/ICAs used.

81,139
average number of internally trusted certificates

7
average number of internal issuing CAs used

Organizations have, on average, 81,139 internally trusted certificates (e.g., certificates issued from an internal private Certificate Authority [CA]) and have an average of 7 internal issuing Certificate Authority's (CAs) that they use across their organization.

Often, legacy PKI solutions cannot meet new use cases and deployment models, meaning that teams are turning to non-compliant methods. Various teams are deploying CAs without gaining the appropriate approvals (shadow IT) – both of which are contributing to vast certificate sprawl. This abundance of certificates being issued by unmanaged and unsanctioned CAs results in higher levels of complexity, fragmentation, and security risks.

Many organizations are also finding that additional resources are required to maintain their infrastructure – which is only adding to the operational burden that many are feeling (see page 19). Having a decentralized PKI, several issuing CAs across businesses without centralized governance, reporting, or management means a clear lack of unified visibility. This leaves organizations unable to identify vulnerabilities or detect unauthorized certificates in many cases. Organizations need clear and consistent visibility into their certificate landscape, without which it's almost inevitable that vulnerabilities will be missed, or outages will occur.

Figure 13:
To what extent do you agree or disagree with the following statements? - My organization would benefit from having more visibility into all issuing Certificate Authorities (CAs) and PKI tools [1200] Showing the combination of those that strongly agree and agree.

92%

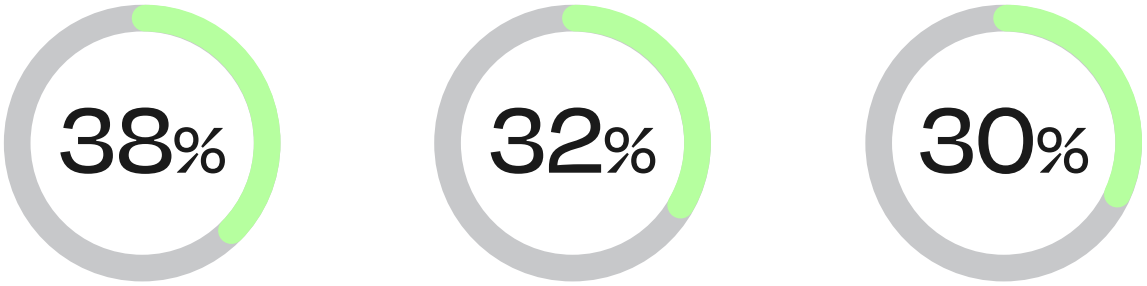
agree their organization would benefit from having more visibility into all issuing Certificate Authorities (CAs) and PKI tools

Effective certificate lifecycle management through dedicated certificate lifecycle management automation software

Figure 14:

How teams primarily track and/or manage their certificates

How does your team primarily track and/or manage its certificates? [1200] Not showing all answer options.



Organizations are lagging behind in the tools they are using to primarily track and manage their certificates, with more (38%) using spreadsheets and homegrown solutions, often a patchwork of open-source tools, databases, and scripts. This is weighing heavily for many, with over 8 in 10 (84%) experiencing an increased operational burden on their teams, and this tough reality is increasing year-over-year (62% in 2021, 70% in 2022, and 72% in 2023).

Organizations that are using a dedicated certificate lifecycle management tool are experiencing fewer outages too – with 17% having experienced zero outages, compared to only 5% of those that use spreadsheets, and 9% of those using homegrown solutions.

Effective certificate lifecycle management is critical for organizations to mitigate the risks associated with certificate sprawl and to ensure the security, availability, and compliance of their digital assets. Investing in a dedicated tool to alleviate the operational burden is a clear action organizations can take to protect and automate machine identities across their businesses. This increases the visibility of their certificates and will streamline their certificate lifecycle management process, reducing vulnerabilities and mitigating the risk of outages and security incidents caused by certificate-related issues.

Figure 15:
To what extent do you agree or disagree with the following statements? - The growing use of cryptographic keys and digital certificates has significantly increased the operational burden on my organization's teams [1200] Showing the combination of those that strongly agree and agree.

84%

agree the growing use of cryptographic keys and digital certificates has significantly increased the operational burden on their organization's teams

WHEN OUTAGES OCCUR

The consequences of inadequate certificate lifecycle management

Figure 16:
Approximately, how many times has your organization experienced the following during the past 24 months? [1200]
Showing the number of incidents.

3

incidents on average, where an **outage** in which an **expired certificate** was the **root cause**

Over the past 24 months, organizations report an average of 3 incidents where an outage occurred due to an expired certificate. This is more evident for those that don't use dedicated certificate lifecycle management software, with those using spreadsheets and homegrown solutions more likely to experience multiple incidents (3 or more) (61% and 57%, respectively, compared to 49% for those using a dedicated tool).

Certificate-related outages disrupt critical services, applications, and systems, which can have far-reaching consequences. It can render systems unusable or inaccessible to employees and customers, which can impact productivity, revenue, customer satisfaction, and even reputational loss.

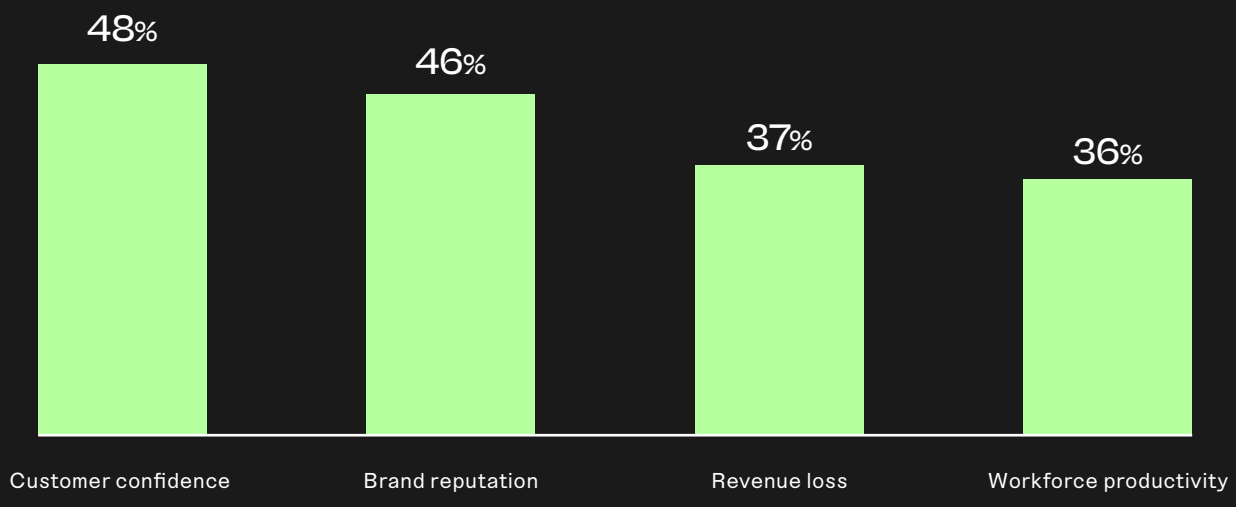
Almost half believe customer confidence would be primarily affected within their organization, alongside many believing that brand reputation would be primarily affected. However, they aren't the only impacts, with revenue loss and workforce productivity being felt by many.

Revenue loss is often cited as the major impact of outages, and it is a primary concern when business disruption occurs. However, it is customer confidence and brand reputation that are the hardest hit, indicating that outages can, and do, impact external-facing systems that are critical to business operations. Typically, customer confidence and brand reputation are intangible assets, and these can also have an impact on an organization's bottom line if lost. Awareness of the impacts that outages can have on customers and how their brand is viewed is vital for organizations to safeguard their business continuity.

Figure 17:

Impacts of an outage caused by an expired or misconfigured certificate

For each of the following scenarios listed, please identify which factors would be primarily affected within your organization. [1200] Not showing all answer options.



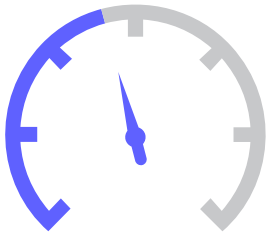
THE COST OF AN OUTAGE

The consequences of inadequate certificate lifecycle management

Certificate outages can incur significant costs for organizations, both in terms of downtime and the resources required to identify and remediate the issue.

The time taken to identify a certificate outage is critical in minimizing its impact on business operations; however, pinpointing the root cause can be challenging and time-consuming, especially in complex IT environments. It takes an average of 2.6 hours to identify one outage, and staff are often diverted from their primary responsibilities to troubleshoot the issue, leading to a loss of productivity and potential delays in other tasks or projects.

Figure 18:
On average, how much time does it take for your teams to identify and remediate one certificate-related outage? Asked to respondents who have experienced at least one outage in the past 24 months or don't know. Showing the average time taken in hours.



2.6 hours

is the average length of time it takes for teams to **identify** one certificate-related outage

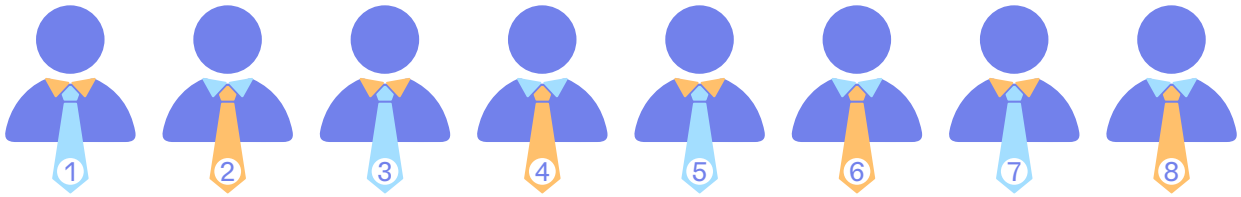
Identity Average [1,047]

2.7 hours

is the average length of time it takes for teams to **remediate** one certificate-related outage

Remediate Average [1,046]

Once the certificate outage is identified, the next step is remediation – including renewing and replacing the affected certificate, and restoring services to their normal operation. The remediation time can vary depending on the outage. However, the average time is 2.7 hours; in addition to the time it takes to identify the outage.



With an average of eight staff members involved in response and remediation during a typical outage caused by a certificate-related incident, this is a considerable expense for organizations. According to a report by Robert Half[4], the average engineer salary in 2024 ranges from $115,000 to $163,00 a year and up to $230,000 a year in major metropolitan markets.

Considering that over five hours is needed for identification and remediation, multiplying this by 8 staff members and their hourly cost for just one outage demonstrates the financial repercussions of improper detection and protection. This is not to mention the other staff involved when an outage occurs, such as customer support or customer service employees. Though not directly involved in the stages mentioned, they are inevitably involved and, in particular, trying to limit the impacts on customer satisfaction and confidence mentioned on page 26.

The 'drop everything' nature of responding to an outage only adds to the burden felt by organizations. And it's predictable that the more certificates an organization has without a clear and integrated certificate management system, the more certificate outages will occur. This will lead to more staff being tied up in identifying and remediating the outages, causing the costs to spiral.

Having a solution to prevent certificate outages will benefit organizations considerably. With less than a third of organizations using dedicated software for certificate management (page 23), this highlights an area where organizations can mitigate the costs and make savings with their time to relieve the burden their IT security teams are experiencing.

4 - https://www.roberthalf.com/us/en/insights/salary-guide/technology

WHEN AUDITS ARE FAILED

The consequences of inadequate certificate lifecycle management

Compliance challenges with certificate management are evident, as without correct supervision, a lack of compliance can lead to compliance violations, audit failures, and legal liabilities, exposing organizations to fines, penalties, and legal consequences; not to mention reputational damage.

Figure 19:
Approximately, how many times has your organization experienced the following during the past 24 months? [1200]
Showing the number of incidents.

3

incidents on average, where a **failed audit** or **lack of compliance** was from **unenforced/insufficient key** or certificate management **policies**

Organizations report an average of 3 incidents where a failed audit or lack of compliance occurred from unenforced/insufficient key or certificate management policies in the past 24 months.

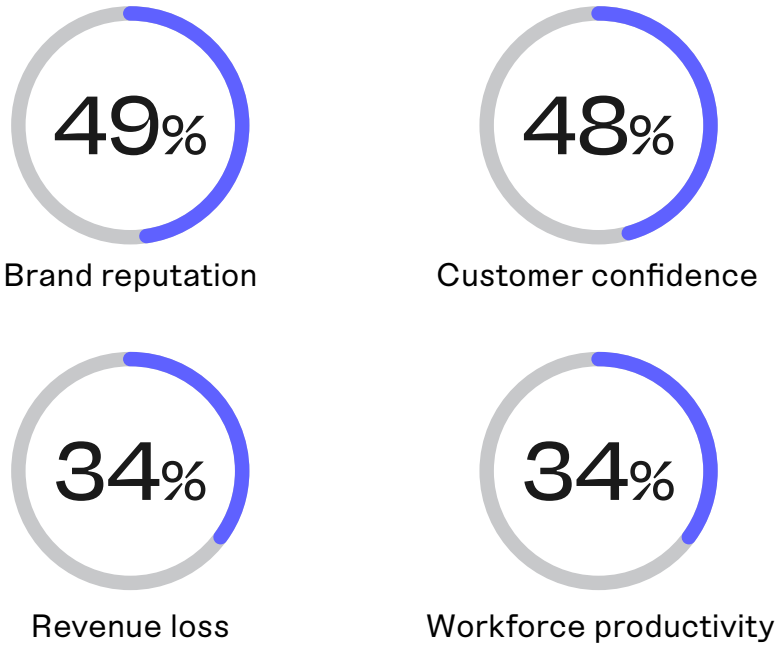
Failing audits can lead to costs in many areas, such as financial penalties, fines, or legal fees, but also costs to remediate compliance issues identified during an audit and carry out corrective actions. Similar to what we saw with outage impacts, the time taken from staff to carry out compliance-based activities can quickly cumulate into high volumes of lost productivity and delays to planned work.

Brand reputation is considered the greatest area impacted by compliance or auditing failures (49%), and tarnishing an organization's reputation will intimately erode customer trust and confidence (48%).

Figure 20:

Impacts of a failed audit or lack of compliance from unenforced/insufficient key or certificate management policies

For each of the following scenarios listed, please identify which factors would be primarily affected within your organization. [1200] Not showing all answer options.



By prioritizing compliance, investing in automated tools and processes, and conducting regular audits and assessments, organizations can reduce the risks associated with noncompliance and ensure the security, integrity, and availability of their digital assets.

WHEN SECURITY INCIDENTS OCCUR

The consequences of inadequate certificate lifecycle management

When certificate lifecycle management is inadequate or improperly managed, predictably there is an increased security risk. Expired or misconfigured certificates, weak algorithms, and unauthorized certificate issuance leave systems vulnerable to cyber-attacks, data breaches, and unauthorized access; the consequences of which are extremely serious.

Figure 21:
Approximately, how many times has your organization experienced the following during the past 24 months? [1200]
Showing the number of incidents.

3

incidents on average, where a **breach** or **security-related incident** was due to **lost or stolen keys or certificates**

An average of 3 incidents have occurred for organizations in the past 24 months where a breach or security-related incident occurred due to lost or stolen keys or certificates. The cost of this can be immeasurable, from forensic investigations, remediation, monitoring, and any compliance breaches and penalties; as well as the other areas we have explored in this section of the report.

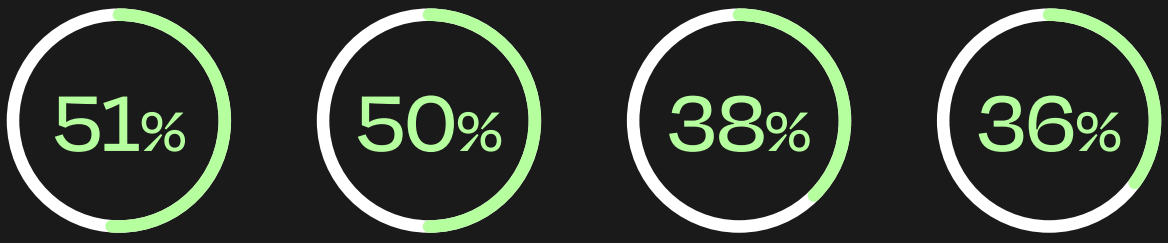
The increased certificate volume inevitably leads to a greater security risk where there are more keys or certificates that can be lost or stolen, and this again presents a vast operational burden in the efforts to identify, remediate, and mitigate the impacts of such incidents. Inefficiencies such as manual certificate provisioning, renewal, and revocation are prone to errors, delays, and inconsistencies, which can lead to more breaches occurring.

With brand reputation (51%) and customer confidence (50%) again the primary factors affected when breaches and incidents occur, organizations must focus on preventative measures to limit the impacts. Implementing access controls, encryption algorithms, and certificate lifecycle management software to protect from unauthorized access or misuse is key. Further auditing and assessing their security posture, providing ongoing training, and cybersecurity awareness for employees will further safeguard against the devastating impacts that breaches can bring.

Figure 22:

Impacts of a breach or security-related incident due to lost or stolen keys or certificates

For each of the following scenarios listed, please identify which factors would be primarily affected within your organization. [1200] Not showing all answer options.



SUMMARY

The consequences of inadequate certificate lifecycle management

In summary, each of the types of certificate management failings discussed in this section has occurred multiple times for all organizations surveyed over the course of a two-year period, each time impacting their brand reputation and customer confidence in particular. Therefore, this is something organizations need to grasp control of to limit the business impacts of inefficient certificate management.

To mitigate potential consequences, organizations should focus on prevention by implementing robust certificate management practices, including automation, monitoring, and auditing. For those that are experiencing vast certificate growth, seeking support from vendors that can provide comprehensive certificate management will help to mitigate the risks outlined.

Top PKI and certificate trends in 2024

Figure 23:
In your opinion, what are the most important trends that are driving the deployment of PKI, keys, certificates, and other secrets? [1200] Showing top 3 answers.

#1 trend

48%
Mobile devices (e.g., BYOD, mobile device management)

#2 trend

46%
Increasing use of AI/ Generative AI technology

#3 trend

46%
Internet of Things (IoT) devices within organizations

In 2024, organizations face a rapidly evolving digital landscape marked by the proliferation of mobile devices within organizations, the increasing use of AI/GenAI technology, and the widespread adoption of IoT devices. As we've seen throughout this report, these often mean an enhanced PKI and an increasing number of certificates required.

The top trend reported for 2024 is the use of mobile devices, such as bring your own device (BYOD) policies and mobile device management. An increasing reliance on mobile devices for business operations means an organization's PKI must adapt to support secure authentication, encryption, and mobile platform usage.

The second highest trend is the increasing use of AI/GenAI technology. As we have seen (see page 9), organizations prioritize this area in their strategies for identity management and are increasingly looking to AI and GenAI technologies to support this. These technologies, however, are still in their infancy. Using AI in certificate lifecycle management, cryptography operations, or certificate usage insights will be key areas for organizations to help improve their security posture and to help manage an increasing certificate load. The more an organization uses AI for *any* business operation, the more machines that organization will need to enable this – all of which will, in turn, need to be authenticated and secured using digital certificates, adding to an organization's machine identity management load.

The third trend for PKI and certificates in 2024 is the use of Internet of Things (IoT) devices. The proliferation of connected devices within organizations presents many challenges for certificate management and PKI, as the volume and array of devices, each with their own security needs, means that organizations need to scale their solutions to meet this increase.

These trends underline the critical importance of adapting cybersecurity strategies and technologies to address evolving threats and technological advancements. By staying abreast of these trends and ensuring they are prepared for vast growth in the number of devices (both mobile and IoT) and the volume of AI/GenAI usage means organizations are less likely to be overwhelmed by the growth in certificates needed and the load to their PKI infrastructure.

The journey to PQC and organizations' preparedness

One major disruption on the horizon for all organizations is the rapid development of quantum computers, capable of breaking some of the most widely-used security protocols in the world today. Organizations are aware of this threat and there is a clear importance for organizations to prepare for this emerging challenge. While some organizations have begun planning for quantum-safe cryptography, many are yet to make strides in their journey.

Only two in ten (23%) organization's timeline to begin planning for PQC planning is a work in progress. Most are waiting for standards to be released or finalized, with over a third (36%) expecting to start in 2024 after the first release of standards happen later this year, and a quarter (25%) are waiting for the standards to be fully finalized. The minority are waiting for quantum computers to be capable of cracking modern encryption or when classical algorithms are deprecated, and very few (2%) say that their organization is not concerned about PQC security.

Figure 24:
My organization's timeline to begin planning for PQC is... [1200]. Not showing all answer options

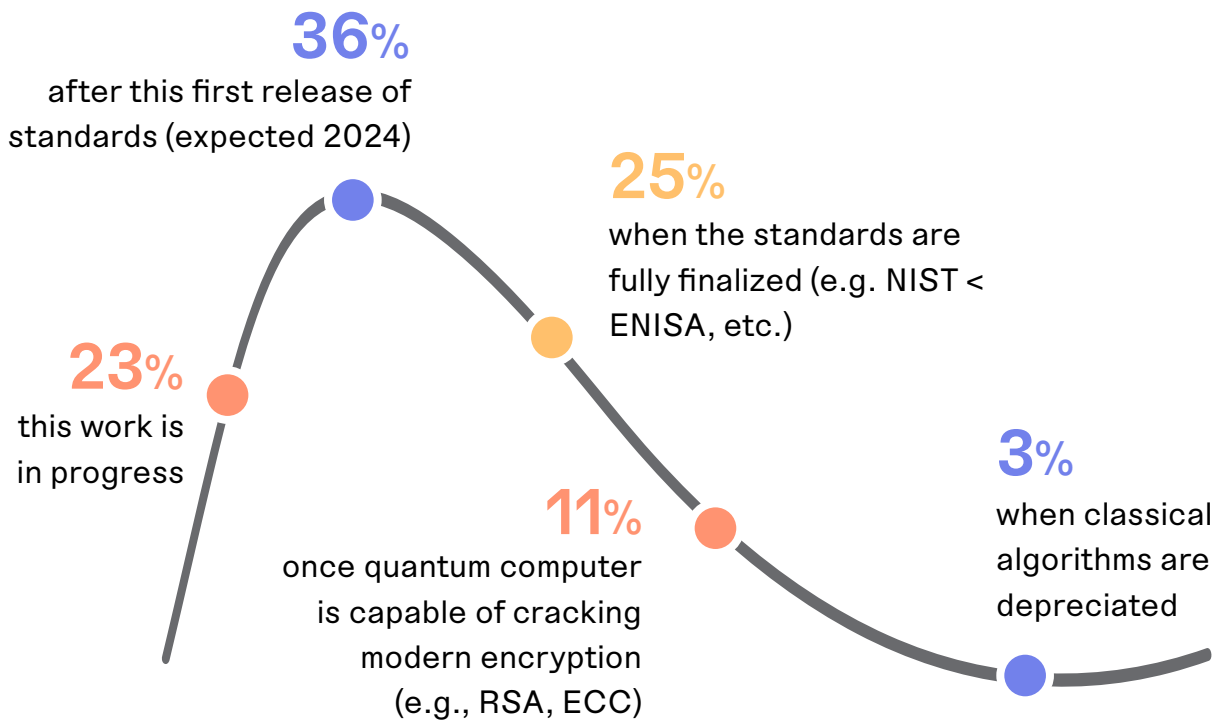


Figure 25:
To what extent do you agree or disagree with the following statements? - My organization is concerned about the ability to adapt to risks and changes in cryptography [1200] Showing the combination of those that strongly agree and agree.

80%

agree their organization is concerned about their ability to adapt to risks and changes in cryptography

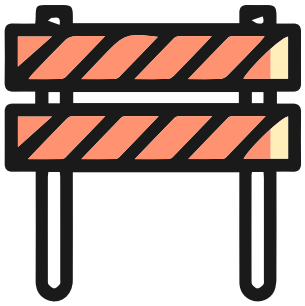
There is a vast amount of work for organizations to do before they can be ready for PQC, such as assessing the impact on their existing cryptographic infrastructure, resolving interoperability concerns, the need for extensive testing and validations, and developing strategies to mitigate the risks. Though it may be some time before quantum computers are able to crack modern encryption (see page 40), failing to prepare for this threat could leave organizations highly vulnerable to attacks that exploit the weaknesses of traditional cryptographic algorithms. The costs of this could be significant.

Many organizations (80%) report they are concerned about their ability to adapt to risks and changes in cryptography, demonstrating that this is top of mind for most IT decision-makers. This concern has increased from 48% in 2023, highlighting the growing acknowledgment that early action is crucial to stay ahead of the curve and maintain the trust and confidence of stakeholders and customers in an increasingly quantum-enabled world.

The challenges associated with PQC readiness

While PQC holds promise as a solution to the threat of quantum computing, organizations face several challenges in preparing for its implementation. Limited budget and resources, integration challenges, and the skills and knowledge required of employees are among the key obstacles organizations must overcome. And with most being in the early stages of their PQC planning (page 36), it's no surprise that most are experiencing these challenges.

Figure 26:
What primary obstacles, if any, is your organization encountering in the process of getting ready for PQC? [1163] Asked to respondents whose organizations will prepare for PQC, not showing all answer options



95%

report their organization is encountering obstacles in the process of getting ready for PQC

Implementing PQC requires significant financial investment to research, develop, and deploy, and with the competing priorities in 2024 (page 35), this is perhaps why organizations are finding it challenging to prioritize PQC in their budgets. Integrating PQC solutions with existing cryptographic infrastructure, applications, and systems will present many technical challenges and compatibility issues that organizations will need to navigate as their teams move toward PQC readiness. This again ties to budgetary and resource constraints as this requires investments in upgrades or custom development to ensure seamless integration.

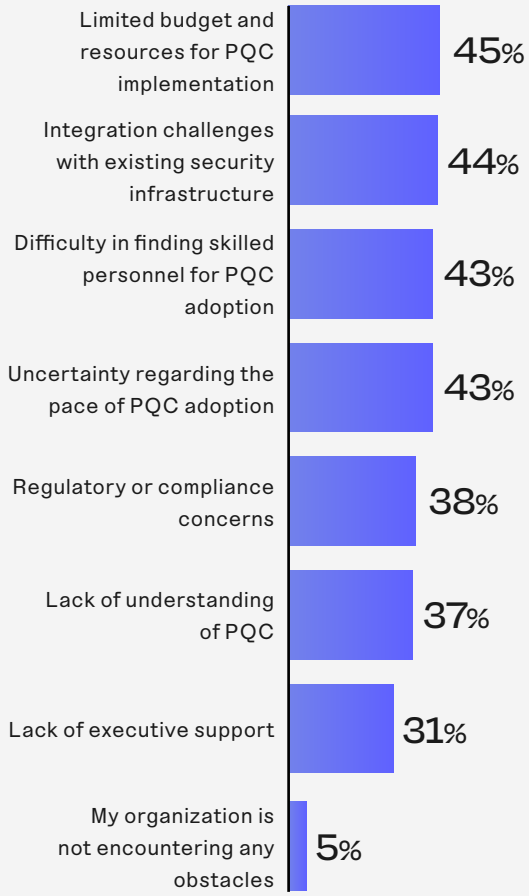
For IT security professionals, less than 4 in 10 (39%) feel very prepared for PQC, which is not surprising, considering the challenges discussed above. For those working closely in the security of their organizations, the focus will increasingly be placed on the future threat of quantum computing. Therefore, the transition to PQC must be prioritized in the organization's strategy, budgets, resource allocation, technology, and hiring to ensure it can move forward.

It is interesting that over a third (37%) report a lack of understanding with PQC. Without a full understanding of what they are trying to achieve with PQC, it will be hard for organizations to be confident in their direction and strategy in this area. This likely ties to the many that are waiting for the PQC standards to be initially implemented in 2024, or to be fully finalized (page 36). With a lack of standardization in algorithms and protocols, it is difficult for organizations to select suitable solutions or security requirements to ensure operability. With potential regulations and requirements not yet in place, organizations must keep abreast of evolving frameworks to ensure their PQC implementation complies.

Figure 27:

Obstacles encountered in the process of preparing for PQC

What primary obstacles, if any, is your organization encountering in the process of getting ready for PQC? [1163] Asked to respondents whose organizations will prepare for PQC, not showing all answer options



Actions that organizations are taking in their PQC journey

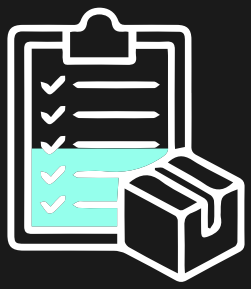
With the concerns and challenges of PQC readiness apparent, organizations are preparing to start their PQC journey by taking various actions.

Developing and ensuring a clear PQC strategy is the top action being taken, which will be key to ensuring a collaborative and comprehensive approach across an organization. Inventorying all cryptographic assets, including keys, certificates, and algorithms, is a crucial early step organizations are taking to understand the scope and scale of the developments required, and this will allow organizations to prepare and prioritize where to focus their upgrades and replacements. Researching and evaluating PQC solutions will enable organizations to identify and assess the tools and solutions that best align with their security requirements and operational needs. Ensuring that challenges are proactively met, and organizations are prepared for the post-quantum era will be essential to ensuring the long-term security of their cryptographic infrastructure.

Figure 28:
What actions is your organization taking, if any, to prepare for PQC? [1163] Asked to respondents whose organizations will prepare for PQC, not showing all answer options

51%

are developing a PQC implementation strategy



49%

are taking an inventory of all their cryptographic assets

49%

are researching and evaluating PQC solutions

While organizations may perceive that they can achieve PQC readiness within a relatively short timeframe, the reality is that the transition to PQC is a long-term endeavor that may take over a decade to complete.

Overall, organizations believe it will take an average of 4 years to transition to PQC, which appears to be an underestimation. Many sources, such as NIST [5], indicate that the timeline for quantum computers being able to break all public keys schemes currently in use is 'within the next twenty or so years,' and The Global Risk Institute [6] reports that experts estimate the likeliness is 10, 15, 20 or 30 years away. In essence, there is no consensus from experts on the exact timing – though with it being a certainty, organizations should be preparing. It is perhaps the lack of understanding of PQC, noted on page 39, that is blocking a full and clear view of PQC, and the timelines required for readiness. Further to this, those with more certificates believe that it will take longer to transition – 6 years, on average. It suggests that those with more to manage will need more support in this transition.

Underestimating the time and effort required for PQC readiness will likely lead to delays, setbacks, and increased security risks as quantum computing capabilities advance. Therefore, organizations must begin their journey as soon as possible.

5 - https://csrc.nist.gov/projects/post-quantum-cryptography
6 - https://www.quantum.amsterdam/part-5-when-can-we-expect-a-useful-quantum-computer-a-closer-look-at-timelines/

Recommendations

Steps to successful machine identity management

In this section, Keyfactor provides steps organizations can take to improve their machine identity management strategy and recommended resources to support these efforts.

Organizations must better prepare for vast volumes to manage

Organizations need to prepare now for the volumes of certificates they have to continue increasing and ensure they have the proper strategy, management capabilities, and software to manage these higher volumes effectively. The risks associated with poor certificate management and certificate sprawl can devastate a business and its reputation; therefore, ensuring these are in place before they become unmanageable is imperative.

IT and security leaders must master the elements of digital trust, which include PKI, PQC, CLM, and code signing, if they want to unlock all the incredible benefits that IoT, cloud, mobile, and AI bring to our now hyper-connected world.

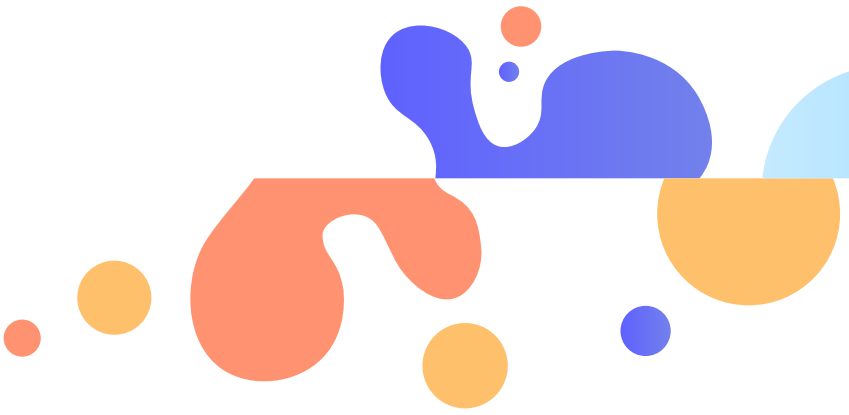
Investing in machine identity management is key

Ensuring that machine identity management is a top priority when considering strategic budgets for 2024 and beyond is key to maintaining and expanding PKI and certificate management capabilities.

Investing in a dedicated solution to provide full visibility, automate certificate management, and manage digital identities at scale will standardize solutions across an organization and alleviate much of the operational burden caused by fragmented solutions or management.

By auditing their machine identity landscape, organizations will be able to determine where gaps exist and where tools and processes can be enhanced, including:

- PKI and certificate management
- SSH key management
- Privileged access management (PAM)
- Enterprise code signing
- Secrets managers
- Key management systems (KMS)
- Hardware security modules (HSMs)
- Managed PKI services



Complexity in PKI infrastructure is holding organizations back

Unexpected outages, failed audits, and security breaches continue to be common occurrences for organizations, with 9 on average experienced by each organization across the past two years.

The management tools being used by organizations are, in many cases, self-reported to be inadequate or fragmented, which has increased from 23% in 2021 to over a third in 2024 (34%). This is only increasing the operational burden teams feel, and 81% agree that the misconfiguration of PKI and certificates is an increasing machine identity management concern.

Reducing complexity within organizations should be a priority for organizations that experience high levels of fragmentation or divisions across different areas of their business. Replacing legacy solutions with modern PKI and automated certificate lifecycle management software will ensure cohesiveness across an organization and allow them to be equipped for the volume and velocity of certificates issued today.

Organizations need to kick-start their journey to post-quantum readiness

Staying ahead of the curve and adapting to changes in the security landscape is vital, and organizations can do this by starting their journey to PQC. Classical algorithms in use today will inevitably be breakable, whether by quantum computers or AI-enabled technologies. Post-quantum algorithms promise stronger security in the face of increasing threats. Organizations must not delay their strategy to inventory, test, and migrate their current processes to quantum-resilient algorithms as they become standardized.

By embracing crypto-agility, organizations should develop a PQC implementation strategy, taking inventory of all their cryptographic assets and researching the PQC tools and solutions that best align with their security requirements and operational needs. Partnering with a vendor that can support PQC readiness will ensure they are proactively preventing the dangers that quantum computing threatens.

Additional resources

Navigating the State of IoT Security

This report explores the challenges of securing IoT and connected products, as well as factors contributing to the vulnerability of organizations using these devices internally: the rapid proliferation of connected devices, the cost of inadequate cyber defense, and the complexity of where liability lies for successful cyber breaches.

Planning Ahead for Post-Quantum Cybersecurity

In this white paper, discover why now is the time for organizations to protect their data and identities from the future threat of quantum computing.

The Role of Digital Trust in an Untrusting World

This white paper examines the importance of building digital trust and how it enables organizations to support new products and business opportunities.

The State of Quantum Readiness Report

This report highlights the top challenges security professionals face when it comes to preparing their organization for PQC, including budget, integration obstacles, and a shortage of skilled labor.

Methodology

Keyfactor commissioned independent market research agency Vanson Bourne to conduct research into the state of machine identity management.

The study surveyed 1,200 IT professionals in January 2024, all of whom worked in organizations that have a Public Key Infrastructure (PKI) and had a level of familiarity with it. Respondents were from the US, Canada, UK, France, Germany, Switzerland, and Austria.

Respondents were from organizations with 1,000 or more employees across a range of public and private sectors, predominantly from the following sectors: IT, technology, and telecoms; industrial and manufacturing; healthcare and pharmaceuticals; energy and utilities; insurance; and financial services.

Respondents were comprised of a range of seniorities, from board members and c-suite respondents, through senior, mid and junior-level management, to those who are technical specialists. All interviews were conducted using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

Keyfactor has in the past worked with other research firms and previously published the State of Machine Identity Management reports in 2021, 2022, and 2023.

This report sometimes references data from the previous State of Machine Identity Management reports. Please note there have been slight wording changes between the surveys, of which full details can be provided if required. Where there are wording differences, we have used the 2024 wording. In addition, the scope has had some changes, so caution has been taken when comparing past data iterations. The main differences include:

- Department: the 2023 report consisted of 1,280 respondents, with 28% IT security/InfoSec respondents, though the departments surveyed broadly aligns with the 2024 survey
- Headcount: The 2023 survey also included respondents from organizations that had fewer than 1,000 full-time global employees (22%)
- Sector: the 2023 report consisted of a slightly different sector list

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed.

For more, visit **keyfactor.com** or follow **@keyfactor**.

Built on a foundation of trust and security, Keyfactor is a proud equal opportunity employer, supporter, and advocate of growing a trusted, secure, diverse, and inclusive workplace.

VansonBourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit **www.vansonbourne.com**.