EBOOK

Three Strategies to Help Security Leaders Navigate the Cybersecurity Labor Shortage

KEYFACTOR

Table of Contents

The cybersecurity world is currently grappling with a significant labor shortage — and that's a problem with serious consequences. The Department of Homeland Security has cited the cybersecurity labor shortage as a major national security threat, and The Washington Post notes that "the dearth of cyber workers is making it harder to protect government data from being stolen by adversaries and diminishing its ability to help improve cybersecurity in industries vital to national and economic security."

Understanding the Cybersecurity Labor Shortage

(ICS)2, an international nonprofit membership association focused on building a safe and secure cyber world through education and skill-based certification, first noted the labor shortage in 2020. The organization's annual workforce study sought to understand the impact of the pandemic on cybersecurity professionals and revealed a need for over three million qualified workers.

Not much has improved in the two-plus years since that report. Keyfactor's 2022 State of Machine Identity Report dug deeper into the impact of this shortage, revealing that 50% of organizations lack personnel in key roles.

This situation is alarming: without the personnel required to properly analyze, detect, and remediate security-related incidents, breaches are *inevitable*. And while the industry is both aware of the situation and taking great strides to fill the personnel gap, incidents are increasing at such a breakneck pace that we've reached the point where it's nearly impossible to simply add more people to provide the necessary coverage.

Fortunately, the future is not all bleak. While it's important to focus on fixing the labor shortage, it's also imperative for organizations to adopt technologies that can help their existing cybersecurity teams work more efficiently. These technologies can go a long way toward resolving the challenges we face today.

50%

of organizations lack personnel in key roles.

2022 State of Machine Identity Management Report

The cybersecurity labor shortage by the numbers

There is a significant shortage of skilled professionals in the cybersecurity industry, and businesses need to understand the scope and scale of the problem if they want to navigate it successfully.

Fifty-percent of organizations say they lack personnel in key cybersecurity roles. In the 8 years from 2013 to 2021, the number of vacant cybersecurity jobs worldwide grew from 1 million to 3.5 million (350%), and despite there being around 1 million cybersecurity professionals in the U.S., there are still some 715,000 jobs that need to be filled.

A shortage of people with the necessary skills required to secure the systems the modern world is built on is a serious matter. The Department of Homeland Security described the cybersecurity workforce shortage as nothing short of "a national security risk." Addressing the problem won't be inexpensive. At a mean base salary of $107,000 per year, bringing on nearly three-quarters of a million more cybersecurity workers will involve substantial investment.

Given how crucial cybersecurity is, it's worth understanding what factors have contributed to the shortage of professionals with the relevant expertise. Here are a few:

The field of cybersecurity is evolving rapidly

New threats, use cases, and technologies must be addressed by the most highly-skilled professionals, and maintaining such a labor force is an inherently difficult task.

Technology is being applied to new business processes

Industrial internet of things (IIoT) manufacturing is a prime example. Though it's a reality today, it would've been science fiction 25 years ago, and keeping such operations running safely requires expertise in manufacturing and supply chains, in addition to cybersecurity.

Technological advancements are finding their way into every industry

From the smallest businesses to the largest enterprise organizations, more companies and industries are deeply reliant on software than at any point in history. Where cybersecurity might have once fallen solely within the purview of a few IT-dependent departments, it has now become a constant concern across companies of all sizes.

The confluence of these forces has created a demand that outpaces the supply of cybersecurity professionals. Insufficient staffing leads to misconfigured systems, less time for proper risk assessment and management, unpatched critical systems, a lack of oversight in processes and procedures, ignorance of active threats against the network, and rushed deployments.

Meanwhile, cyber-attacks make headlines daily. Even businesses that have never taken security seriously must pay attention to organized cybercriminals taking hospitals and banks to the cleaners for staggering amounts of money and sensitive information.

The consequences of these mistakes are costlier than ever. The average cost of an enterprise-level breach rose from $3.86 million in 2020 to $4.24 million in 2021 to $4.3 million in 2022. In 2021, 60% of small businesses that experienced an attack went out of business within six months. Furthermore, attacks on infrastructure and utilities have the potential to endanger the lives of millions.

Given how crucial security has become and how badly underserved it is, what can organizations do?

Addressing the Shortage — Should You Invest in Talent, Tools, or Infrastructure?

What we mean by "addressing the shortage" is really "how do we address the growing cybersecurity workload?" In other words, encouraging more people to enter the field is a possible solution, but it may not be the only one.

Even if there were already enough talent in the marketplace, it is expensive to scale your personnel at the same rate at which systems are becoming more complex, threats more common, and technology more diverse—especially if team members are using manual, outdated workflows that monopolize their time with rote, repetitive work and prohibit them from focusing on higher-level objectives.

The cybersecurity labor shortage by the numbers

There's no point in optimizing something you shouldn't be doing in the first place, such as maintaining some badly outmoded system. Unfortunately, it's often the case that when a business process is digitized, it merely replicates the manual process in a virtual space rather than rethinking and remodeling it from first principles to leverage the advantages of a digital approach.

But modernization isn't a cure-all. Sheer workload and system complexity create a drag on your team's productivity.

A report from the Ponemon Institute surveying over 1,000 security leaders showed that there's only so much a single person can accomplish, no matter how sleek and new your tools are.

- 46% of respondents said a single staff member could be responsible for managing between 4 and 10 tools.
- An additional 11% said one staff member could be responsible for handling more than 10 tools.
- 50% said they use at least six different tools to respond to the average security incident.
- On average, it takes teams 17.7 hours to respond to an average security incident.

Investing in your infrastructure gives you the most bang for your buck

Infrastructure investments empower security professionals to focus on the highest-level work and either eliminate out-of-control manual tasks or make it possible to shift this work to less-technical team members.

Of the three most common solutions—adding more people, adding more tools, and investing in infrastructure—only the last is subtractive. Investing in infrastructure lets you declutter your systems and processes and achieve the kind of lean, efficient, capable operation that can ultimately be managed with fewer highly-skilled individuals at a lower total cost of ownership.

Three Strategies to Help Your Team do More with Less

01 Streamline certificate lifecycle automation

Why put so much emphasis on certificate lifecycle automation? Your security team probably doesn't have the bandwidth to manage certificates adequately, on top of their other priorities, and the costs of mismanagement are extremely high.

Since the 1990s, asymmetric cryptography has been the standard for securing connections with web servers, email, network administrators, and more. Until around 10 years ago, enterprises commonly employed an internal PKI team to manage these functions. But with the cloud, remote work, IoT devices, DevOps, and other evolutions, the volume and prevalence of certificates has exploded.

Keyfactor's 2022 State of Machine Identity Report revealed that enterprises have an average of 269,562 public and private certificates.

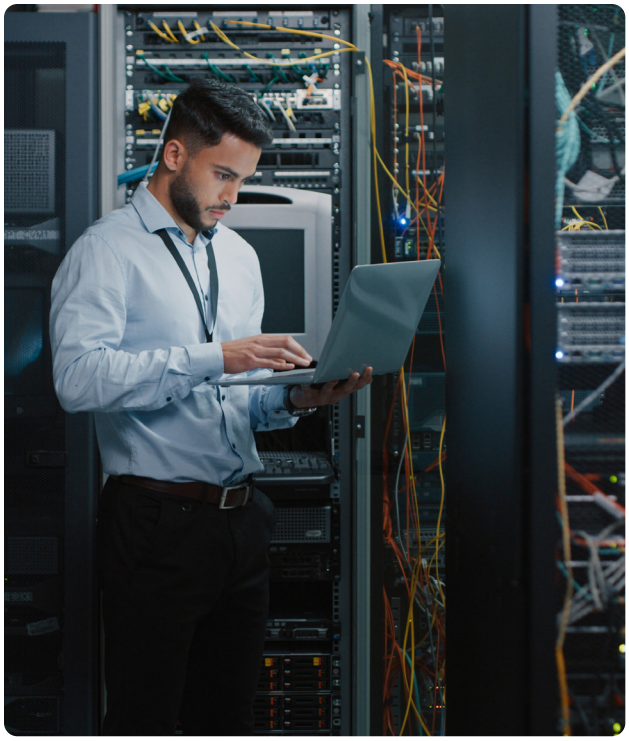
That's a lot to manage! In the past, most enterprises had dedicated teams for managing certificate lifecycles, but organizations gradually shifted certificate management duties to the general security team. This is not ideal, as security teams rarely have machine identity expertise and are not typically suited or staffed to manage PKI alongside their many other priorities.

Only

44%

of organizations use a dedicated certificate lifecycle management solution to track and manage certificates

2022 State of Machine Identity Management Report



The extent of the problem is clear from survey results.

- Only 50% of organizations said they had adequate staffing for managing certificates.
- 70% of respondents said that increased use of keys/certificates has significantly increased the operational burden of the teams managing them.
- 42% are making do with spreadsheets, and 33% rely on labor-intensive homegrown tools.
- 67% said a certificate-related outage took more than three hours to identify and remediate.

Mismanaging certificates can have massive, negative consequences. Some of the most high-profile incidents in recent memory, such as SolarWinds and Epic Games, involved compromised digital certificates. Among the most stark occurred when the US government shut down in 2019. Because no one was updating the SSL and TLS certificates for government websites, dozens of them were simply inaccessible, leading to a number of serious security issues.

And the regulatory landscape adds a significant layer of complexity. Regulations governing certificate-related security not only differ from region to region, but they are also constantly evolving and expanding. Certificate lifecycles, meanwhile, are getting shorter, requiring more frequent updates and thus more work for your team.

As if that wasn't enough, quantum computing and other emerging technologies are forcing organizations to make certificate management a higher priority. But how can you possibly handle all this in the midst of a cybersecurity labor shortage? Enter a scalable certificate lifecycle automation solution.

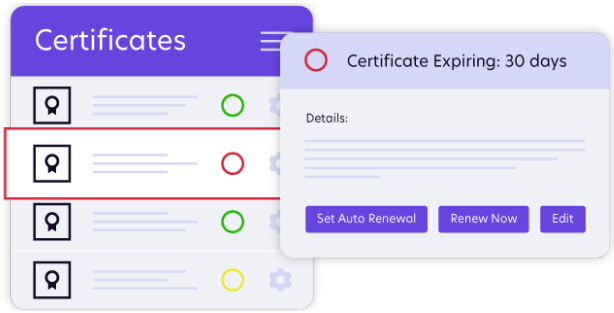
Embrace automation with a CLA solution

As the number of keys and certificates multiplies across your business, odds are you'll face a number of challenges, including a lack of visibility and manual, error-prone processes. When PKI and security teams get stuck in reactive mode, they're forced to focus on outage response over strategic security initiatives. Teams can shift from being in reactive response mode to proactive visibility and automation with an end-to-end automated public key infrastructure (PKI) and certificate management solution like Keyfactor Command.

An automated solution enables PKI and security teams to scale certificate lifecycle management without diverting staff or other resources. In addition, they'll gain:

Visibility through centralization

Gaining visibility into the state of certificates across the enterprise immediately eliminates the person-hours required to manually hunt down certificates. A certificate lifecycle automation platform creates an audit trail, which reduces time spent trawling systems to compile reports.

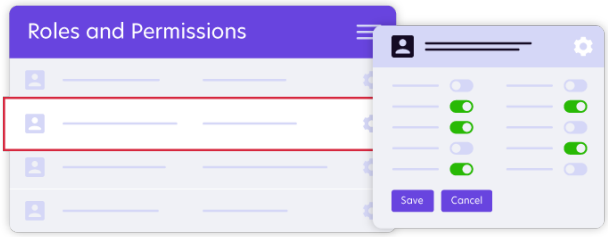


Security through speed

PKI and security teams can see cert expirations coming before they happen and automate the creation and issuance of new certificates. This drastically reduces the inefficient back-and-forth usually required to request, create, deliver, and implement a new certificate. More broadly, it prevents costly downtime and outages.

Quality through standardization

A unified hub for managing certificates and machine identities also serves as a single source of truth for guidelines, ownership around certificate management responsibilities, and best practices.



For these reasons, many organizations use their certificate lifecycle automation solution as a foundation for their internal machine identity management working group. When used in this way, the group defines ownership, lays guidelines for using machine identities, and establishes a strategy for the future.

Given the "total cost of ownership" of your existing certificate management processes, the efficiencies created by a certificate lifecycle automation solution could provide the ROI needed to support a dedicated team, whether that means converting existing staff or hiring additional team members.

Alternatively, you can tap into a vendor with deep certificate management expertise to take these duties off your security team's plate, in whole or in part. This can free them up to focus on other tasks, reducing the need to hire more security staff.

02 Embrace the cloud

The cloud has long been a pillar of the digital transformation movement, and a common goal of digital transformation: Doing more with less. Security is no exception, and the cloud is a source of several security efficiencies, including:

An extra layer of protection

Cloud providers take on much of the infrastructure maintenance, monitoring, and updating, which removes that burden from your team. Cloud providers encrypt data, automatically provide backups, and monitor their own firewalls. Major cloud providers meet the most common accreditation standards like PCI 3.2, NIST 800-53, HIPAA, and GDPR.

The best cloud providers monitor activity continuously, in real time. They can aggregate data across various users to better recognize patterns of suspicious behaviors and threats. They may deploy algorithms and machine learning tools that monitor your team's typical pattern of activity and flag events that fall outside the norm.

A centralized and simplified infrastructure

Rather than accumulating a patchwork of security tools to fit each individual device or server, a cloud-native security stack brings consistency and simplicity to your toolkit while improving your security posture. With cloud-based tools, you can push out updates and patches remotely.

Additionally, in an on-prem model, you must build out resources to meet peak demand, and you maintain and pay for those resources, even when you're not consuming them at a peak rate. With the cloud, you share that burden with other cloud customers, along with other costs like backups, resiliency, and availability.

Forward-thinking tools with SaaS-level support

Cloud-first tools and vendors tend to be more forward-thinking. They facilitate agile operations, prevent vendor- and tool-lock, streamline your toolkit, integrate with other systems and programs, provide a range of service options, and offer flexible deployment for on-prem, cloud-only, and hybrid infrastructures.

With the cloud, you have the choice of outsourcing highly-technical niche functions if they're business-critical but not business-central. Working with a specialized vendor gives you greater operational efficiency than hiring these resources and building these infrastructures in-house.

PKI and certificate management are prime examples

Typically, you can only deploy one certificate authority per server. When development, IT, and other departments want different certificate authorities, this leads to sprawl.

Keyfactor can run an entire PKI system on one instance, reducing dozens of servers down to just a few—or even one in some instances—drastically simplifying your landscape while lowering costs. Keyfactor provides a database and native integrations, so you don't have to shop around at a ton of other vendors. Keyfactor even helps you migrate your existing certificate management infrastructure to the cloud.

With Keyfactor, you can self-manage your PKI on Keyfactor's servers or offload certificate management entirely to Keyfactor's experts, freeing up your team to handle higher-level tasks.

03 Prioritize retention

Hiring more cybersecurity professionals is likely a top priority, but don't forget to retain your current staff. It's basically guaranteed that current employees are at least casually paying attention to the myriad opportunities for higher pay, career advancement, or better working conditions brought about by the Great Resignation and a high-demand job market.

Understanding your team's perspective

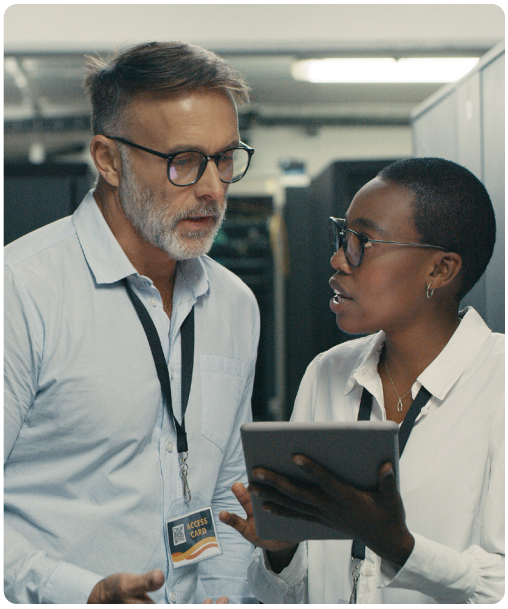
To aid retention of talented employees, it's important to think about things from their perspective. What are some of the factors which might push them to go elsewhere?

They are burned out

The pandemic has done a lot to exacerbate what was already a widespread problem with feeling stressed and overworked. In addition to the broader Great Resignation trend, the pandemic drastically accelerated digital transformation. While this was a boon for many businesses, cybersecurity workers bore much of the brunt of that push. According to a VMware report, 51% of cybersecurity workers admitted they were feeling burnout, and 65% considered leaving the profession altogether.

They do not feel like leadership "gets it"

Today, many cybersecurity teams are challenged to "do more with less." According to research from CyberArk, senior security professionals (79%) agree that security has taken a back seat to maintaining business operations. Plans to "do more with less" rarely include substantial investments that help cybersecurity teams be more efficient (and less stressed).



They can be discouraged by high-level outside hires

Your team takes note when all managerial and higher-level positions are filled externally. They may interpret this as a lack of opportunity for upward advancement.

Build loyalty among your team

All this headache can be avoided by making your organization a place where your team feels like they can shine, succeed, and advance without burning out or spending their time on tedious manual work. What concrete steps does this involve?

Listen to their needs and become a champion for them

Try to understand your team's workflows, so you can see their pain points for yourself. That way, you can advocate for tools, investments, and changes to their processes that deliver real value by eliminating manual work and empowering them to focus on higher-level tasks.

Further, work to understand the skills gaps in your team and the exact risks facing your organization. That way, you can hire with precision and avoid bringing someone on who is ill-equipped to do the job.

Burnout is a real threat to your cybersecurity staff. Be sure to build in recovery time after periods of high-pressure work, like incident response.

Create pathways for career advancement

About 50% of cybersecurity workers started in IT and transitioned to security—transitions facilitated by the fact that 91% of organizations were willing to pay for the training and certification of employees.

Allow time for your team to get up to speed on new cybersecurity practices and skills. Ninety-one percent of cybersecurity professionals believe this is a must for staying effective at their job, but 59% said their job requirements left no room to upgrade their capabilities.

Remember that the ramp-up time is long. Sixty percent of organizations said it takes between 2 and 5 years for a cybersecurity professional to become proficient in a new role, but once you create a pipeline, you can future-proof your team against the next labor shortage.

Bridge the gaps in conversation

Collaboration is a foundational concept of Agile, DevOps, and Digital Transformation, but it's also simply good business practice. Looping your security team into conversations about planning can remove security as a bottleneck to innovation.

Security and IT staff need help developing their business acumen, and they need more insight into the business strategy so that they can offer higher-value recommendations. Conversely, C-suite leaders need enough technical understanding to adequately define objectives and hold realistic expectations.

What's true vertically is also true horizontally. Security doesn't just fall on your cybersecurity team—everyone plays some part in keeping your organization safe. As you implement cloud strategies, endpoint protections, and other security initiatives, try to over-plan the amount of training needed to get engineers, operations staff, and business users to a point of proficiency before beginning the next phase of your transformation.

Staying ahead of today's challenges while practively planning for tomorrow

Organizations today must contend with serious cybersecurity challenges, like constantly evolving threat vectors and the proliferation of machine IDs with increasingly shorter lifespans. According to a global report from CyberArk, machine IDs now outnumber human ones in the average organization by a factor of 45x.

Luckily, there's a lot leaders can do to address these challenges while also navigating a labor shortage. PKI as-a-service is a cloud-based solution that combines expert-managed PKI and certificate lifecycle automation into a single, cloud-delivered platform. It frees enterprises from worrying about day-to-day security operations while still allowing them to maintain control and ownership of the security elements. Laying the groundwork for a PKI strategy now can help you mitigate the labor shortage, and it will make life easier for your existing staff by introducing automation and centralization to a manual process.

Getting ahead of escalating threats marks your organization as forward-thinking and proactive, which is appealing to both current staff and potential new hires. And the cost savings made possible by an automated solution gives you more resources to invest in staff and tools, inspiring loyalty in your team.

In 2022,

71%

of organizations suffered a successful software supply chain-related attack that resulted in data loss or asset compromise

CyberArk, 2022 Identity Security Threat Landscape Report

Build the Business Case for Modernizing and Automating PKI

Here are five steps to build a business case for modernizing and automating PKI and converting your certificate lifecycle management practice from manual to automated.

1

Bring in the A-Team

Work with the system and network admins who are managing your PKI certificates to learn how they're obtaining their certificates and how much time it takes to provision, install, and renew them.

2

Map out the process and identify your gaps

With your A-Team, map out your CA infrastructure, applications, and certificate workflows (including requests, issuance, and renewals). This will help you identify gaps and inefficiencies.

3

Define your project requirements

Once you've identified the problem, outline an ideal solution, what it would take to achieve it, and whether you've got what you need in-house or if it requires a new tool. Remember to avoid limiting this to a single use case (which frequently happens with PKI teams). This should be a solution for certificate management now and in the future.

4

Know what you're up against

Security and risk management leaders are often unaware of the scope or status of their X.509 certificate deployments. These unknowns leave you unequipped to do your job. Even if you haven't experienced a SEV1 outage, you need to clearly communicate the risks and operational costs of outages and certificate vulnerabilities in your network.

5

Nail the ROI

Avoid budget limitations by highlighting how much money can be saved over the next five years by paying the upfront costs of purchasing the solution. In these estimates, be sure to point out how much additional productivity will be gained by removing the need to spend hours manually managing certificates.

Making the right investments

The writing is on the wall: Cybersecurity is growing from a business need to a business demand — especially in a global labor shortage.

To meet the challenge of tomorrow's threat landscape, leaders must have realistic expectations and strategy-backed priorities for their teams. Competing priorities can lead teams to overwork yet underperform. Once priorities and duties are aligned, leaders must discern which levers will deliver the greatest impact and efficiencies for that team.

In other words, what should your PKI or security team be doing, above all? How can you implement processes and solutions that clear their deck of everything else, and what investments can you make to simplify the processes they are responsible for?

If the security strategy is aligned to the greater aims of the business—enabling scale, maximizing risk coverage, and cutting costs—then security will begin to work in harmony with other business functions, such as innovation, rather than in conflict. Eliminating the burden of certificate lifecycle management is low-hanging fruit for immediate gains in efficiency, security, and morale among your internal team.

Enable Scale | Maximize Risk Coverage | Cut Costs

Ready to learn how a complete certificate lifecycle automation strategy can benefit your organization?

Get in Touch

Get started on your journey to modernize PKI, request a demo from a Keyfactor expert

Request a Demo

On-Demand Demo

See end-to-end PKI & certificate automation in action, watch a demo now

See it in Action

KEYFACTOR

Keyfactor is the machine and IoT identity platform for modern enterprises. The company helps security teams manage cryptography as critical infrastructure by simplifying PKI, automating certificate lifecycle management, and enabling crypto-agility at scale.

For more information, visit www.keyfactor.com or follow us on LinkedIn, Twitter, and Facebook.

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.

Contact Us

- www.keyfactor.com
- +1.216.785.2946