

 ebook

Cyberworkforce Shortage

SteelCloud[®]



How to Beat the Cyberworkforce Shortage

Across the US and all its industries, the [Bureau of Labor Statistics](#) notes that we have 11.3 million open jobs, yet only 5.9 million unemployed people. Meanwhile, in the security sector, there are over [700,000 unfilled positions in cybersecurity](#), with an unemployment rate of nearly zero. While US job openings remain near record highs, the unemployment rate is at a two-year low of 3.6%, and wages have been boosted at a healthy clip. So, two things are going on here that impact every profession in the country—the supply of workers is low and wages are rising.

Adding to the issue in the cybersecurity sphere is another pair of challenges—the soul-sucking character of the work and the lack of apprenticeship programs. Navigating Security Technical Implementation Guides (STIGs), Center for Internet Security (CIS) benchmarks, and Cybersecurity Maturity Model Certification (CMMC) to secure infrastructure is not something someone just out of college can do. You are left with highly skilled experts doing mind-numbing work until they burn out. That's not good for your recruiting efforts.

What results is a perfect storm for our national security—increasing attacks and a decreasing number of people to thwart them.

Leaders are making huge security decisions as the economy fluctuates.

The global cybersecurity market is expected to grow at an annual rate of 9.5% a year, reaching almost \$375 billion a year by 2028, according to [Vantage Market Research](#). That's about double the rate of growth forecast for overall IT spending, at least over the next two years, according to [Gartner](#). Price and wage inflation, along with a cyberworkforce shortage, is causing cybersecurity organizations to make impossible choices amid growing threats as the rise in the adoption of IoT surges.

[Cybereason](#) is a cybersecurity technology company whose business is up and whose prospects are bright. But [inflation and the growing costs of cybersecurity professionals](#) have caused them to lay off [10% of their workforce](#). It's a vicious cycle. Cybersecurity budgets are expanding due to inflation and demand, so companies reduce their workforce when workers are at a premium.

As the leaders of [Lacework](#), who also laid off workers, states, "While we do not have control of the environment around us, we do have a responsibility to control how we operate our business and make changes as needed to best position the company for continued and long-term success."

In contrast, at [Illumio](#), whose software helps prevent ransomware and stops breaches from spreading across networks, CEO Andrew Rubin said the topic of downsizing or letting people go "was not on the agenda". Other billion-dollar companies like Snyk and Tanium are not even thinking of slowing down when it comes to hiring.

Regardless of how you might judge the decisions of these companies, the current supply and demand issues don't just impact the companies and the lives of their cyberworkforce; they impact the security of our nation's data.



Cyberworkforce shortages are causing leaders to rethink employment strategies.

In recent years, a steady supply of [cyberattacks](#) targeting government agencies, financial institutions, health care, and other vital sectors have demonstrated the country's vulnerabilities in cyberspace. They also showcase a lack of trained IT security professionals, alarming experts who have spent years tracking the growth of hacker groups.

"The cybersecurity talent shortage is one of the most significant and threatening challenges facing our industry today. We all need to think differently about the problem," said Barbara Massa, executive vice president at the cybersecurity firm Mandiant. "We need more cyber professionals entering the career field. And a cybersecurity career should be within reach for anyone who wishes to pursue it. We need more pathways to cyber careers, and we need them as soon as possible."

Examining the cost of cybersecurity on its workers.

There are many reasons to pursue a [career in cybersecurity](#). Across the board, cybersecurity roles offer abundant employment possibilities, competitive pay, growth opportunities, job security, exciting day-to-day tasks, and the chance to make a difference.

But what if your day-to-day is neither exciting nor fun? What if, instead, it consists of long days and much stress? The work environment can be nerve-racking and overwhelming if you are a security engineer, CISO, or security analyst working in security compliance. With the rise in [data breaches](#), [cybercrime](#), and [workforce shortages](#), it's enough to make anyone anxious and on edge.

As technology rapidly evolves, so do the tactics used by cybercriminals, adding an underlying layer of stress to the work of protecting the nation's infrastructure and networks. Add in the frustration of spending your time doing repetitive manual tasks, like when meeting STIG and CIS compliance requirements, and people burn out quickly. This, in turn, significantly impacts the cyberworkforce shortage.



We need more cyber professionals entering the career field.

Barbara Massa,
Executive Vice President, Mandiant



Taking a look at life in the cyber trenches.

In today's cybersecurity work environment, no one will ever have enough money for compliance. There will always be enough money for the underlying security, but will there be enough people for it to be fully effective? For the foreseeable future, [today's cyberworkforce challenges](#) will leave even the best funded organizations shorthanded.

We searched the internet to see how that is leaving cybersecurity professionals thinking and feeling and what we saw amused and saddened us:

- ✓ "Crying in meetings mostly. But in all seriousness, it's a large privately held company that never really thought about infosec but is trying to get investors and is facing audits, so it decided it needed a CISO who hired me. I'm building the team, guiding a bunch of projects and herding cats."
- ✓ "I drink a lot, my back and shoulders are shot, my eyes suck, and I don't sleep. I do get paid a lot, though."
- ✓ "I don't get paid fairly for what I do. I actually wish they got a real threat attacking their systems so I can say 'I told you so as I walk out to enjoy the flames from the outside.'"
- ✓ "We have a lot of ground to make up. Adversaries are outpacing us faster than ever it seems."
- ✓ "Not CISO, but in a similar situation. Can relate. Don't drink but, I'm overweight."
- ✓ "Went from architect in infrastructure to Infosec a few years back after solving a bunch of security related issues there only to inherit a million more."

What you see in every one of those anecdotes is stress. The work they love has—because of workloads, company processes, or the nature of the industry—caused them physical and personal issues they didn't expect. And, sooner or later, most (if not all) of them will leave their jobs for something less stressful. Like air traffic control. Or lion taming. And the cyberworkforce shortage will continue.



Automation makes the workforce fonder.

What if there were a way to cut out a lot of the stress and annoyances while leaving the culture you enjoy intact? Automation can help with that.

For example, let's look at automating just the merge of SIEM and eMASS data and having both methods match your checklists, automated systems, and logs because sound rulesets and policies ensure the processes are running effectively, efficiently, and easily for analysts. As a result, something that used to take 100% of your time (and patience) now takes 20% of your time and leaves you free for tasks only humans can do.

[Today's eMASS](#) subsystem enables system owners to record asset information on servers, workstations, network devices, etc., and upload applicable scans and Security Technical Implementation Guide ([STIG](#)) checklists. eMASS automatically applies a "mapping" of STIG items to security controls such that any STIG item not implemented will result in a corresponding security control being labeled as non-compliant.

SteelCloud worked with the DoD to reinvent the cumbersome effort needed to complete and load STIG Viewer Checklist data into eMASS. There are four significant areas where automation can be applied to provide a real advantage to the operationalization of cyber compliance within the DoD:

1. Automate and reduce the effort/errors in merging non-technical CKL data with machine-generated technical data
2. Automate and simplify the production and input of compliance data into eMASS
3. Automate and reduce the effort to produce, name, and store a fully populated STIG Viewer Checklist in bulk (by the 1,000s)
4. Provide complete CKL data to [SIEM](#) data feeds so that complete compliance data is easily accessible through integrated enterprise dashboards

As you can see, this alone drastically reduces the time it takes to merge, scan and store compliance data. [The automated part of eMASS compliance](#) is the rote procedures that drive professionals up the wall and cause stress, so everybody wins.

Another significant benefit to automating [eMASS is accelerating your RMF accreditation](#). Loading STIG Viewer Checklist data into eMASS is burdensome. Still, it gives you a comprehensive view of your manual and machine configuration management and cybersecurity checklist, which is extremely valuable for [RMF accreditation](#).



Using automation to solve the workforce crisis

As professionals in every industry and job description will tell you, a job isn't just a job. And if it is, you're not doing it right. It is an integral part of our lives from which we derive pride and fulfillment. A good job makes us feel good about ourselves. And a lousy job makes us want to leave.

Amid [a workforce crisis as bad as we are in](#), employers would need to clone employees out of nothing to have the resources required for compliance. And that's essentially what automation does—it takes your employees and multiplies their efforts. For example, [SteelCloud's ConfigOS](#) hardens STIG and CIS system level controls around an application stack within minutes, removing months from your RMF accreditation timeline. It keeps systems secure from the lab to production and reduces system hardening time by 90% and costs by 70%.

Using automation to speed the security process will also help you [achieve authority to operate \(ATO\) in hours, not weeks](#). Now, one person can do the scanning and remediation work of an entire team.

Uncovering the hidden staffing benefits of compliance automation.

The path to learning a professional craft has always been complicated, from manufacturing to cybersecurity. Traditionally, you might go through an apprenticeship program or learn from a master. Then you'd get poached by another company happy to pay more for already-trained specialists. And the workforce shortage continues with the supply of high-priced specialists not meeting the demand.

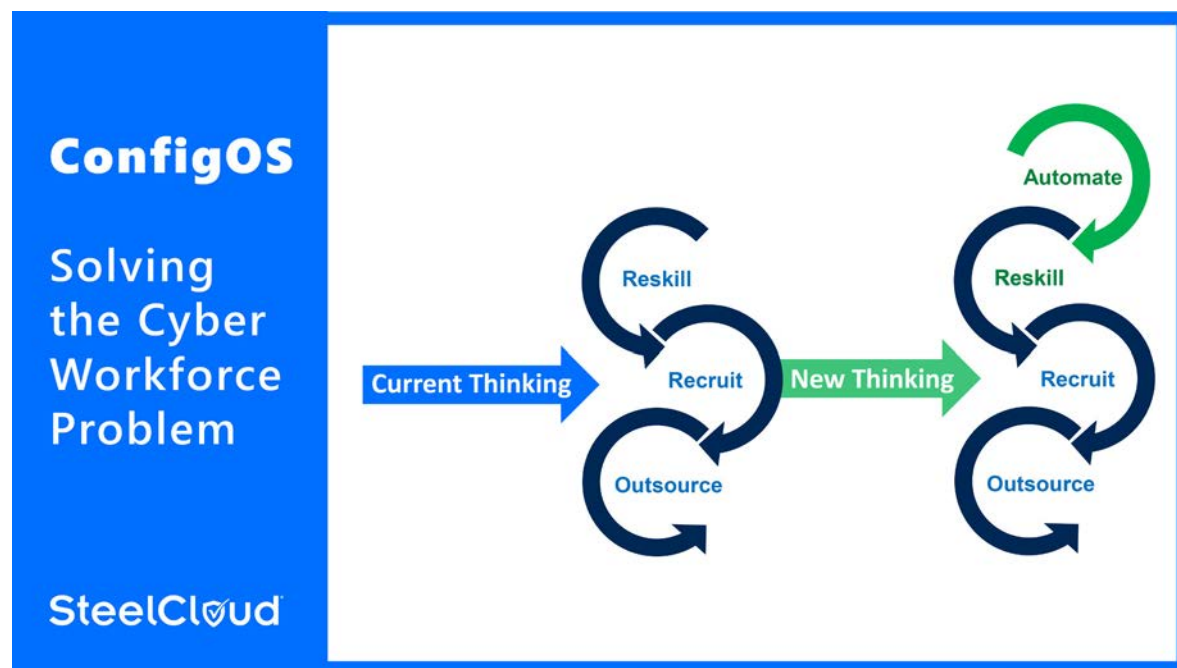
When it comes to government cybersecurity, the path is even more arduous. You could get a master's degree in cybersecurity and still not know how to [STIG](#). There are no trade schools to introduce you to the craft, either. The only way to learn is to work alongside an expert, passing the knowledge down from generation to generation. And anyone who has ever STIGed before will tell you—that it's a long process to learn a crappy job that you will likely leave after a few years because it has sucked out every drop of life left in your soul.

There is a way out, however. As you may know, you can use automation to scan and remediate STIG, [CIS](#), and [CMMC](#) controls, thereby removing the tedious aspects of manual STIGing. Better yet, automation solutions like [SteelCloud's ConfigOS](#) cut weeks and months of manual work down to about an hour, speeding you to ATO and strengthening security.

But there are other, more big-picture aspects to automation that you may not have considered. For example, it's not just about robots doing the undesired work of humans. Instead, it's a way to shift your reskilling and recruiting processes so you can [solve the cyberworkforce issue](#) for your organization for good.



Rethink the way you reskill your workforce.



Traditionally, we reskill a workforce with training and mentoring. It takes time and effort. It generally [takes 3-5 years for a cyber worker to become proficient](#). But even finding someone to train to STIG is difficult because you want some experience. [With a deficit of 714K cyber workers](#), finding someone game to learn the work of compliance security is difficult. And it's also challenging and expensive to have one of your experienced employees' productivity compromised by having to train the new guy.

[Automation can change all that](#). Instead of training recruits to STIG, you train them to operate a robot. It takes a couple hours. With SteelCloud's ConfigOS, we have seen low-level cybersecurity workers then train themselves on the intricacies of STIG/CIS/CMMC compliance, remediating controls, and next steps just by operating the software. They become STIG ninjas in about a month. Then, if they ever go back to manual STIGing, they are better off having worked with automation. They know the process. They have seen the use cases. They understand the fixes.



Changing the way you recruit and use your resources.

As things stand now, if you need more resources for compliance, you pay a hefty price to get them. With job vacancies at an all-time high, it's a job seeker's market. For the most part, recent college graduates don't want to start their careers with this kind of work. And experienced workers are in top demand. The hardest job you can give your recruiters is looking for someone with compliance experience who wants to work for you.

Automate the compliance work, however, and you can recruit lower-level employees with fewer skills to work at lower wages—not to do the grunt work, but to operate the automation software while working on other priorities. So, instead of a repetitive, mind-numbing job manually STIGing, they have an exciting job learning new things and doing various cybersecurity work.

Need a whole team of STIGgers? Just wash, rinse, and repeat to clone your capabilities. Compliance automation makes your cybersecurity team infinitely scalable because the robots doing the work can take on virtually any number of security controls during their 24/7/365 shifts. They won't complain. They won't make demands. And they don't make mistakes.

In short, automation can cause you to fundamentally rethink how and whom you recruit for these cybersecurity positions. And it can help your recruiters shift from "this %&\$#@ workforce shortage!" to "what workforce shortage?" with just a simple install of compliance automation software.

Addressing the cyberworkforce shortage with automation changes EVERYTHING.

Whether you use it for eMASS or STIG compliance, [automation is the only viable answer to the cyberworkforce shortage](#). It gives your well-educated, highly paid experts a break from work beneath them. And it provides organizations a faster, less expensive, and more accurate way to achieve compliance. But, best of all, it makes work fun again. And in the end, that will ultimately grow the industry and its supply of qualified workers.

Automation doesn't replace the work people value. As a result, it addresses the work people don't want to do—exacting, tedious work with consistent rules. Automation creates a balance where machines do what they do best, and humans do what they do best. And that, in turn, gives you the bandwidth and budget to get more done. "Automating STIG and CIS security measures go beyond relieving your IAs to address patches and backlogs," states Brian Hajost, CEO of SteelCloud. "ConfigOS simplifies recruiting and retraining efforts, preserves budget and, with everyone on the team appropriately challenged by their work, also goes a long way with retention."

With a growing cyberworkforce shortage, inflation, and record numbers of Baby Boomers retiring, [something's got to give](#). Compliance automation neutralizes those issues and allows you the opportunity to rethink your reskilling and recruiting strategies for a more prosperous and sustainable pipeline of cybersecurity professionals.

Cybersecurity is an ever-changing landscape of threats, challenges, and innovations that requires adaptable, problem-solving thinkers and doers. Let SteelCloud help you address the workforce shortage and the rising cost of professionals and training with SteelCloud's industry-leading solution, ConfigOS.



About SteelCloud

SteelCloud develops STIG and CIS compliance software for government and commercial customers. Our products automate policy and security remediation by reducing the complexity, effort, and expense of meeting government security mandates. SteelCloud has delivered security policy-compliant solutions to enterprises worldwide, simplifying implementation and ongoing security and compliance support. SteelCloud products are easy to license through our GSA Schedule 70 contract. SteelCloud can be reached at (703) 674-5500 or info@steelcloud.com. Additional information is available at www.steelcloud.com.