

Whitepaper

Navigating critical challenges facing modern CISOs

The challenges facing today's CISOs may seem insurmountable, but a sensible and smart approach can still provide defenders with the upper hand against modern threats

Executive summary

The job of a Chief Information Security Officer (CISO) is becoming increasingly difficult as both technology and those who would attack it become more complex and sophisticated. In addition to that, competition for skilled cybersecurity workers is fierce, with millions of security jobs unfilled worldwide. Meanwhile, legacy systems that are too integrated or expensive to replace keep limping along, bringing old vulnerabilities and aging security problems with them into the modern era.

All of that can make a CISO's job seem almost impossible, which is why the burnout rate is so high in that field. But while the challenges are difficult, they are not impossible to surmount. By tapping into innovative best practices that can turn the tide and give the advantage back to the defenders, overworked CISOs can finally sleep a little easier.

Introduction

Perhaps no job in recent history has evolved more in a short period of time than that of a CISO. In the not-too-distant past, a typical CISO was mostly seen as part of the IT staff, someone who directed IT workers and planned cybersecurity defenses, but who was not really a part of a company's upper management, and had little to no impact on the core business.

However, a long and never-ending string of high-profile breaches and the fact that the threat landscape has become more dangerous than ever before has served to elevate CISOs to upper management in organizations of all sizes. Many CISOs now have a seat on the board of directors, and a well-earned place in the C-Suite of the companies and organizations that they serve. Their contributions are now directly tied to the core business, because no modern company can operate without its computing infrastructure that drives both business operations and customer interactions.

But with great power comes great responsibility. While many CISOs now have a say in things like budgeting for cybersecurity, the threat landscape they are facing is also expanding and evolving. The latest Verizon Data Breach Investigations Report for 2022 clearly shows a threat landscape that is more dangerous than at any other point in history. The CrowdStrike 2022 Global Threat Report paints an equally grim picture, with an 82% increase in both data leaks and ransomware attacks compared with last year.

\$3.8 Million

is the average cost
of cleaning up a
cybersecurity breach

Attacks are also increasing in sophistication, with 62% of attacks going into 2022 belonging to the malware-free category, which is designed to focus on credential stealing to avoid detection from legacy antivirus products and other traditional cybersecurity protections. Another report from Picus Security showed that many attackers were also becoming proficient in 100% fileless attacks, which are very difficult to detect, much less defend against. And the attack patterns and targets are also changing, with many threat actors choosing to invest their resources into supply chain attacks and double extortion operations on top of their normal practices. All of that is making successful attacks more costly. The Cost of a Data Breach Report from IBM and the Ponemon Institute put the cleanup costs of a cybersecurity breach at an average of \$3.8 million per incident.

And if all of that were not bad enough, CISOs are facing an unprecedented shortage of skilled cybersecurity personnel at a time when they are sorely needed. In the United States alone, about 1.1 million people are employed in cybersecurity—but there are also more than 700,000 unfilled job openings.

Without enough skilled cybersecurity professionals, competition for top talent is fierce, and most firms can't afford to pay the kind of salary that top cybersecurity professionals demand.

The factors combine to make things rough on CISOs, despite their new-found respect and role inside most companies. In fact, stress levels and burnout rates are higher than ever for those in a CISO role. A [recent study](#) by executive search firm Heidrick and Struggles found that 59% of CISOs surveyed reported high levels of stress, and 48% admitted to contending with burnout.

It's clear that the challenges facing CISOs in 2023 are dire. But they are not insurmountable. At [Secure Code Warrior](#), we help CISOs and others overcome those kinds of challenges every day. We have seen what works and what does not, and have come up with paths that can lead CISOs and the organizations they serve out of the dangerous cybersecurity jungle. By investing time and resources in key areas, CISOs can help to level the playing field, protect their organizations, and lower their stress levels.

Key ways CISOs can lower stress and improve cybersecurity

Build loyalty, invest and upskill existing cybersecurity personnel

The lack of skilled cybersecurity personnel is being felt everywhere regardless of geography or business sector. Cybersecurity Ventures estimates that this disturbing trend will continue to grow, resulting in [3.5 million unfilled cybersecurity jobs worldwide by 2025](#).



CISOs looking to hire top talent will need to compete with a plethora of other firms looking to do the same thing. Needless to say, this lets cybersecurity workers pick and choose where they want to work, and command incredibly high salaries that most firms are unable or unwilling to pay. CISOs looking to compete in that environment are in for a lot of stress, and likely quite a few losses, when trying to hire new cybersecurity personnel. The new business trend where CISOs are given great leeway in how they control and spend their budget does little good if everyone they can find to hire is too expensive.

One thing that CISOs might not at first consider as a way to overcome this challenge is to look at their existing workforce as a potential way to improve their security posture. Companies in the past didn't often spend a lot of resources on the existing talent within their organization, even though there are a lot of advantages to adopting that strategy. It was just easier to keep hiring more people from outside to fill in critical gaps. These days, that is no longer an option, or at least not a very cost-effective one.

Instead of competing for people against other companies, smart CISOs are learning about the value of the people who already work for their organizations. Perhaps those existing employees are not already highly skilled cybersecurity professionals, or they might even work outside of IT altogether. But with the proper training and support, they could be eased into critical new roles in cybersecurity.

Firms that create or modify a lot of their own software likely already have a perfect and untapped security resource: their developer community. Developers write software for a living, so many also have a genuine understanding of how computers operate and ways that code can be exploited and manipulated. And many have at least some interest in security. The recent Secure Code Warrior [State of Developer-Driven Security](#) survey found that the overwhelming majority of programmers saw the value of cybersecurity, even though only 8% said that creating secure code and keeping vulnerabilities out of programs was easy. Most also stressed a willingness to learn more about cybersecurity.



Firms that create or modify a lot of their own software likely already have a perfect and untapped security resource: **their developer community.**

Upskilling for a firm's existing developers might involve making a few key changes. For example, instead of simply mandating security to developers, consider creating or appointing security champions from the community. These would be talented and security-aware developers who distinguish themselves either in training or as part of newly focused metrics evaluations.

They should also be willing to help other developers enhance their skills, thus improving the development community from within. Getting developers onboard with security programs is an increasingly effective and cohesive approach to better cybersecurity, and can be done using your existing workforce.

And depending on how great the need is, don't be afraid to look even farther afield for existing employees that are ripe for upskilling. Certainly, entry-level IT workers who are good at their jobs are perfect candidates for advanced training. But other non-IT workers might also be a good fit. For example, someone who works as a security guard may be great at looking for suspicious activities, and a secretary may be well-versed at keeping incredibly complex and fluid executive schedules organized. Any of those skill sets could help a person transition into a new cybersecurity role. Even previous jobs or experiences might make someone a good candidate for deep IT training. Many firms are discovering that the hard and soft skills taught in the military make [veterans a great choice](#) when looking for someone to support in developing cybersecurity skills.

Training up existing personnel, or providing new roles and opportunities for your already hard-working developers, has advantages beyond mere manpower considerations. Taking a good employee working as a developer, or even someone working in a completely different field, and training them to be a cybersecurity professional is incredibly rewarding, not just for the company but also for the employee. The company gets another skilled cybersecurity staff member, but the person doing the training is able to start a whole new career that likely pays a lot more than their previous position, and exists in a field where there is no shortage of opportunities to climb even higher. Employees plucked from other jobs and trained in cybersecurity also tend to become fiercely loyal to the company that gave them the opportunity, so the turnover rate among internally-trained workers is much lower than those brought in from the outside.



Employees plucked from other jobs and trained in cybersecurity also tend to become **fiercely loyal to the company** that gave them the opportunity, so the turnover rate among internally-trained workers is much lower than those brought in from the outside.

Upskilling and training existing personnel makes for a great option for many companies, and can also help relieve a critical area that contributes a lot to a CISO's stress level.

Learn how to deal with legacy systems that can't yet be removed or replaced

If there is one constant in IT, it's that technology is constantly changing. Computers, programs, and peripherals tend to get more advanced, more complex and more efficient over time, often bringing in new capabilities that make the old ways of doing business obsolete. Sometimes entire infrastructures change, such as with the current move away from physical data centers and on-prem equipment into the cloud, something that [48% of major companies](#) recently surveyed said that they are either considering for the future or actively doing right now.

And that innovation is, on the whole, a good thing. For example, the reason cloud computing is so popular is that if done right, a company's data and applications can be safely stored in the cloud and accessed from anywhere in the world without having to support an internal, physical infrastructure. It also allows for unlimited expandability as needs grow, and could potentially cut costs as well.

The problem, however, is that very few companies are starting out from zero. Many have long and established histories and infrastructure, including legacy equipment, frameworks and tools that have become deeply integrated into their operations. This means that, in reality, those continuously changing network dynamics in pursuit of digital transformation usually happen without retiring at least some legacy systems. And keeping those legacy systems protected and up to date makes for one more huge stress point for overworked CISOs.

48%

of major companies recently surveyed said that they are either considering for the future or actively moving to the cloud now.

One of the most egregious examples of this is the use of the COBOL programming language, which was created over 60 years ago. Back in the 1960s, COBOL was like today's Java or .Net, and integrated into the fabric of many computing platforms, especially for business or financial applications. Those who initially coded those applications have long since retired, and yet their programs live on at thousands of companies worldwide. CISOs are charged with protecting and maintaining those applications alongside the most modern applications running in hybrid clouds and using modern frameworks. If that was not bad enough, skilled cybercriminals will almost always look for the weakest link when trying to infiltrate a network or steal data, and those old frameworks, applications and infrastructures are often preferred targets. For example, a modern attack like an SQL Injection can work just as easily in COBOL, even though the legacy program or gear running it likely has less protection against it.

Ideally, replacing legacy gear and applications is probably the best solution, but is not always technically possible without a lot of downtime, or may be too expensive an endeavor to undertake right away. Because of that, smart CISOs should ensure that security teams know how to support and maintain those legacy applications to prevent them from becoming the weakest link that attackers are seeking.

Investing in a platform that recognizes the importance of an advanced training regimen that covers a wide gamut of programming languages is a good way to ensure that security personnel can get up to speed using modern, hands-on training techniques and courses. CISOs can then support deep training for their IT teams relating to COBOL and other legacy languages alongside some of the most modern programming tools available today, like Google's Golang. Nothing gets left behind, even those aging legacy systems that really should have been retired long ago.

Invest in the right kind of training that employees want and need

Poor, check-the-box type of training programs where employees watch a video and enter a few pieces of data have tainted the value of training in the minds of a lot of executives. Particularly for complex fields like cybersecurity, weak, non-interactive, hands-off type of training does little actual good beyond checking a box to show auditors or regulators that mandatory training has been completed. From a CISO's perspective, it does nothing to actually increase security or improve cyber maturity levels. Most of the time, it also accomplishes next to nothing to protect a company's data, assets or customers.

92%

of developers said that getting security training was important. But they want and need good training that speaks to them and **provides hands-on examples.**



But the problem is not the concept of training itself, but the poor quality of the execution. Most people realize that they need good cybersecurity training, especially if they work in IT. In the [Secure Code Warrior State of Developer-Driven Security](#) survey, 92% of developers said that getting security training was important. But, they want and need good training that speaks to them and provides hands-on examples, not a compliance exercise that only wastes their already limited time.

CISOs should strive to ensure that their developers receive meaningful training pathways that provide value, raise code quality, and deliver the kind of content and knowledge that ultimately drives an organization's security maturity. For example, they should look for a firm with a [dedicated training laboratory](#) that constantly seeks feedback from those who use their platform and revises its curriculum with the most modern teaching techniques alongside the latest technical information.

They should also use a training platform that embraces highly efficient training methods like [tiered learning](#), where topics are broken down into discrete educational objectives and concepts. A tiered learning approach then adds newer, more advanced concepts layered on top of those already mastered.

Education can also be the key to supporting many other security efforts, such as the aforementioned programs where members of the existing workforce are brought into cybersecurity roles. But that won't work with substandard training, so this has to be one area that is critical for CISOs to champion if they want to protect their organizations, provide the detailed information their employees crave, and reduce even more stress from their own careers.

Create a security-first culture

The final component needed in order to both improve security and make a CISO's job a little easier does not directly involve technology at all. But it's also been described as one of the most difficult things for many organizations to achieve: a change in culture. It might be difficult, but to truly create an organization where security is top of mind and everyone contributes to that effort requires a security-first culture.

CISOs, with one foot in management and the other over with the rank-and-file IT and security teams, are in a unique position to spearhead the effort to change an organization's culture because it requires both a top-down and bottom-up approach.

Getting upper management on board might be the more difficult of those two objectives. Most C-Suite leadership outside of the CISO and CIO will likely look at business objectives and profits before anything else. It is the job of the CISO to show other executives [a direct correlation](#) between better, more mature cybersecurity and increased revenue, market share and how better security can provide a boost against the competition.



CISOs, with one foot in management and the other over with the rank-and-file IT and security teams, are in a **unique position to spearhead the effort to change an organization's culture** because it requires both a top-down and bottom-up approach.

This can be done in a variety of ways, such as demonstrating to executives [the costs](#) in both dollars and reputational loss that comes from an avoidable cybersecurity breach, and also how the company can use its best security practices in order to assure customers, suppliers, and partners, that their personal data is valued and protected. Once executives start to see cybersecurity as a business driver instead of a complex operating expense, they will be much more receptive to supporting a shift to a security-first mindset and culture.

Once the executives are on board, CISOs can then begin to ingrain security in everyone else at their organization. Developers in particular should be courted since they are in a unique position to shift security towards the [so-called left](#) as far as possible by writing secure code that is free from vulnerabilities and resistant to attacks as soon as it is created. This can be done in a variety of ways, with one of the best being to create security champions directly from the developer community to advocate for security, explain the personal and professional advantages of learning to write secure code, and act as a coach and cheerleader to help bring other developers into the fold.

According to [Gartner](#), the best security champions from development communities are organized and proactive, enthusiastic about security, work well in collaborative environments and possess many other traits that match up with AppSec professionals. Developers will listen to those champions because they are part of the same community, and in fact are also active programmers working alongside them. And with the support of management backing up those efforts, everyone in the organization will be able to see the advantages of the cultural shift towards security.



Changing an organization's culture won't happen overnight, and might even be met with resistance or fear at first. But it's absolutely essential that CISOs keep working at it until that happens.

Changing an organization's culture won't happen overnight, and might even be met with resistance or fear at first. But it's absolutely essential that CISOs keep working at it until that happens. The threat landscape is too complex, too advanced and too ubiquitous for any one person or even a small team to handle alone. True security these days requires the assistance of everyone from the CEO to developers, and on to the people who work in the mail room. Only by having everyone aware of the importance of cybersecurity and actively working towards it within the realm of their role will an organization have a real chance of avoiding costly breaches and downtime, or at least minimizing and mitigating the impact of any attacks that still get through.

Conclusion

The job of today's CISO may seem almost impossible despite the increased influence, respect and inclusion in board meetings that many are now enjoying. And the deck certainly seems like it might be stacked against them, with millions of unfilled security jobs, an increasingly dangerous threat landscape, problems with legacy equipment and unprecedented technology changes and digital transformation.

However, CISOs are also now in a unique position to solve these problems for their companies, further cementing their value within their firms. By investing in existing staff, embracing proven cybersecurity training, learning to tame legacy applications and working to instill a security-first culture and mindset, CISOs can turn the tide against all those negative factors and put their organizations into a good position to be able to thrive despite facing so many challenges. And, it will certainly make meeting the mission-critical objectives of a CISO a little bit less stressful, giving them a much-needed and well-deserved rest from the constant pressures of their rewarding but challenging career.

Please visit [Secure Code Warrior](#) for more insights about cybersecurity issues and protections, and to learn how Secure Code Warrior can help your organization embrace secure coding practices to better protect your software, company, employees and customers.

About Secure Code Warrior

Smarter, faster secure coding

Secure Code Warrior builds a culture of security-driven developers by giving them the skills to code securely. Our flagship Learning Platform delivers relevant skills-based pathways, hands-on missions, and contextual tools for developers to rapidly learn, build, and apply their skills to write secure code at speed.

Established in 2015, Secure Code Warrior has become a critical component for over 500 enterprises including leading financial services, retail and global technology companies across the world.

[Request a demo](#)

[Try Secure Code Warrior for Free](#)



**SECURE
CODE
WARRIOR**