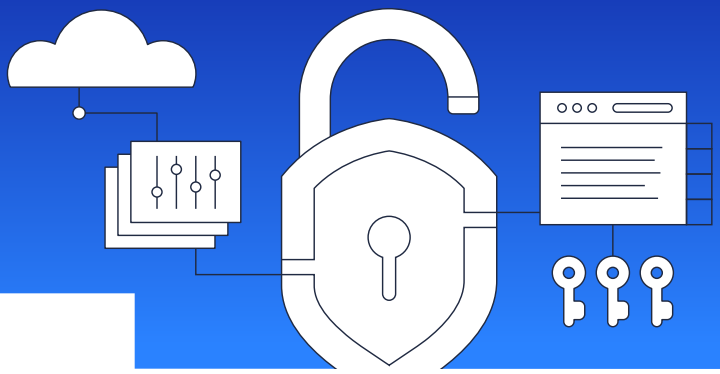
SECURE CODE WARRIOR



ANALYSIS

Benchmarking Security Skills: Streamlining Secure-by-Design in the Enterprise

No other single dimension of 'secure by design' efforts are as consequential as improving the skills and tools of the people that innovate, develop and disseminate code at the heart of digital systems delivering critical services for every facet of our daily lives. Giving developers precision training in secure coding is a good first step toward producing better software. However, demonstrating that they have absorbed those lessons can put a company on the fast track toward a new standard of software excellence and proven Secure-by-Design compliance.

Executive Summary

Finding objective data on the success of Secure-by-Design initiatives is notoriously difficult. CISOs are often challenged when attempting to prove the return on investment (ROI) and business value of security program activities at both the people and enterprise levels. Beyond localized measures of merit, it's particularly difficult for enterprises to gain insights into how their organizations are benchmarked against current industry standards.

The President's National Cybersecurity Strategy challenged stakeholders to "embrace security and resilience by design." More comprehensive, granular insights into key parts of an enterprise and application security program are fundamental to its continuous improvement, and to remain consistent with the now-widespread Secure-by-Design movement popularized by CISA, which has published pivotal guidelines on the subject.

Authors:

Dr. Matias Madou, Ph.D., CTO & Co-Founder, Secure Code Warrior

Pieter Danhieux, CEO & Co-Founder, Secure Code Warrior

Contributors:

Kemba Walden, President, Paladin Global Institute, and formerly acting US National Cyber Director

Chris Inglis, Former US National Cyber Director, now Strategic Advisor to Paladin Capital Group

Special Thanks:

Catie McHugh

Jean Louis Sibert

The key to making Secure-by-Design initiatives work is not only giving developers the skills to ensure secure code, but also assuring the regulators that those skills are consistently employed. In the context of software developers, "upskilling" focuses on enhancing an individual's security performance. It aims to improve (1) individual competency, (2) proficiency in using approved tools, and (3) the methods of establishing and maintaining effective oversight and administration of the software development process by development managers and security leaders.

The end goal for organizations is to ensure that "Secure-by-Design" principles are prioritized and achievable for each software deployment. This approach empowers developers to proactively address security concerns and deliver more secure software solutions. Prioritizing security in developer training can ensure that (a) the people working with an organization's most sensitive repositories have the security skills they need and (b) those who have not heeded the call for security excellence are prevented from accessing key assets. Ideally, making security training a requirement before a developer can access key assets improves the overall security of an enterprise.

While these measures have traditionally been particularly difficult to achieve at the enterprise scale, the insights provided by Secure Code Warrior's "Trust Score" technology open a new frontier of actionable security insights and benchmarking. It is these insights that are crucial for organizations to break free of the ineffective cycle of reactive security, instead embracing a preventative, precision approach that ultimately fortifies the digital infrastructure of the business.

This effort cannot be delivered by relying on bottom-up initiatives. Security leaders are a key element achieving meaningful change. They must provide AppSec professionals and developers with the upskilling and education to integrate security into the beginning of the development process. Once accomplished, security leaders must show that those efforts have taken hold and in fact made applications and data more secure. Only then can chief information security officers and their organizations prove the value of security excellence more clearly, effectively demonstrating positive ROI from investing in cybersecurity.

In this research paper, we share qualitative and quantitative data, derived from multiple primary sources, including internal data points collected from over 250,000 active developers, data-driven customer insights, and public studies. Leveraging this aggregation of data points, we aim to communicate a vision of the current state of Secure-by-Design initiatives across multiple verticals, specifically the Critical Infrastructure Sectors as identified by CISA. The research paper details why this space is currently underutilized, the significant impact a successful upskilling program can have on cybersecurity risk mitigation, and the potential to eliminate categories of vulnerabilities from a codebase.

Introduction: What is Secure-by-Design, and Why Do Developers Matter?

Cybersecurity as a discipline—and the industry it serves —is dynamic. Like most pillars of the technology landscape, it has seen change and evolution at a blistering pace in just a few decades. The '90s was certainly the "virus era", with most cyber incidents coming in the form of malware, worms, and other citizen-targeted malicious software packages. This led to the growth of a $2 billion antivirus industry, as experts in the field began mobilizing to not just respond to the next virus on launch, but predict what threat actors would exploit next.

Taher Elgamel, a cryptographer and mathematician formerly of Netscape, correctly predicted that once online transacting truly hit mainstream, cyberattacks and their potency would increase exponentially: "Most of the time you wait and say 'there are viruses, so let's go catch them' – but we actually predicted that once e-commerce got on the open Internet, that attacks would increase and attackers would want to have a ball playing with the transactions and private information floating over it." As told to Cybersecurity Ventures.

That $2 billion industry is small change compared to today, where it is estimated to have grown to a $2 trillion, multi-discipline landscape, thanks to an insatiable demand for digital-first products and services, as well as most enterprises shifting to a process of continuous digital transformation.

There is more code being produced than at any other time in history, more devastating cyberattacks threatening our sensitive data and national security, and yet, too many companies are trying to protect themselves and their customers with outdated security programs, and too few personnel dedicated to building and maintaining secure software architecture.

That is why security experts worldwide see CISA's 2023 release of Secure-by-Design and Default Guidelines as a watershed moment.

In the modern era, every company is a software company.

Over forty years ago, industry started to adopt digital solutions for purposes of realizing new efficiencies in their business models. Over time, the discipline of computer engineering evolved and the market demanded a new cadre of software developers. We have been experiencing a digital transformation ever since. It has only been within the last 20 years, however, that companies are now also contending with software security.

While most banks still have a significant brick-and-mortar presence in their respective locations, today, they are, at their core, software development companies. JPMorgan Chase, for example, boasts a cohort of 43,000 software engineers, each of whom would be writing code. In addition, most banks buy and deploy software from third parties like Microsoft, bolstering a large cohort of developers who write proprietary software.

This is digital transformation in action, and it is now common across all industries and companies. Energy companies do not simply buy software off the shelf and deploy it; they have a considerable number of software developers who write their own code and integrate it.

Ultimately, almost every company has become a software company in some way. However, few organizations have successfully implemented security controls that have kept pace with the deluge of code being produced, leading to movements like "shift left" that have attempted to correct this by implementing security measures as early as possible in the software development lifecycle (SDLC).

For years, organizations have grappled with the challenge of integrating security into the beginning of the SDLC, butting up against cultural resistance among developers, security, and operations teams, as well as other hindrances ranging from weak access controls to disagreements over the right tools to use. At the same time, organizations of every size and character are trying to improve security amid a persistent global security skills shortage that has essentially become endemic, leading to a high rate of burnout among overworked AppSec professionals.

The Biden Administration's National Cybersecurity Strategy threw down the gauntlet in 2023, saying it is time to "rebalance the responsibility to defend cyberspace." This can be accomplished by taking the burden off the shoulders of individuals, small businesses and local governments, and then shifting it onto the "organizations that are most capable and best-positioned to reduce risks." In other words, software vendors.

The strategy echoes regulatory regimes, such as Europe's General Data Protection Regulation (GDPR), whose principle of accountability is meant to ensure compliance with its Data Protection Principle.

Accountability continues to be a sticking point

High-level accountability could spur companies to invest more in security, but within organizations themselves, there remains the challenge of consistently creating secure code and the question of who is responsible for it. Code ownership is hard to determine as software goes through stages of creation, updating, monitoring, and testing.

As the United States National Cybersecurity Strategy points out, an inability to adhere to secure coding best practices also leads to lax development processes. The constant pressure to rapidly develop and deploy new applications and services leads to companies shipping software with known vulnerabilities, default configurations, and unvetted third-party code.

The release of the national strategy was quickly followed by a seminal speech by CISA Director Jen Easterly, calling for "radical transparency" about the security of software products and for vendors to take responsibility. Easterly also heralded CISA's Secure-by-Design principles, which offer, for the first time at this level, guidance on ensuring that products incorporate security at the start of development.

In short, the game is afoot. CISOs must help create an organization-wide security culture, starting with the SDLC. They need a new playbook to instill that security-first mindset in the creation and use of software code. They should also train and upskill AppSec professionals and developers in secure coding practices, and use state-of-the-art measurement tools to ensure education efforts are taking hold across the board.

Developer upskilling is critical to Secure-by-Design success

"Upskilling", in the context of software developers, specifically relates to their security performance on an individual level. However, this is not an undertaking that developers should be expected to initiate in isolation from their organization or team. The security program should offer, as part of its robust Secure-by-Design strategy, a three-point plan to effectively impart the skills, knowledge and tools to write secure code from the beginning of the SDLC.

Ideally, this would cover:

- Direct education and assessment opportunities to measure and improve individual competency;
- Approved tooling that is matched with the tasks and tech stack required of the developer;
- Oversight and management of the software development process to ensure Secure-by-Design is front-of-mind and achievable for each deployment.

Secure-by-Design as a movement and action

CISA's Secure-by-Design movement has gained significant momentum, with governments around the world - like Australia, New Zealand, Canada, Singapore, Japan, Germany and the UK - contributing to its creation or, indeed, following it directly as part of their own publicized cybersecurity strategies. They have also released advice in a push for more software manufacturers to adopt memory-safe programming languages, essentially eliminating nasty buffer and integer overflow vulnerabilities.

These guidelines represent a sound framework for software vendors to improve the effectiveness of their security programs. However, two key focus areas in their secure product development advice will be difficult to achieve without the right data points to inform a skills benchmark among an enterprise development cohort, and they are:

- **"Provide secure defaults for developers:** *Make the default route during software development the secure one by providing safe building blocks for developers For example, given the prevalence of SQL injection vulnerabilities causing real-world harm, ensure that developers use a well-maintained library to prevent that class of vulnerability Also known as "paved roads" or "well-lit paths," this practice ensures both speed and security, and reduces human error."*

- **"Foster a software developer workforce that understands security:** *Ensure that your software developers understand security by training them on secure coding best practices Further, help transform the broader workforce by updating hiring practices to evaluate security knowledge and working with universities, community colleges, bootcamps, and other educators to weave security into computer science and software development curriculums."*

The current culture doesn't promote developer-driven security, and with little relevant training and impact on their KPIs, the traditional motivators to inspire action are lacking. Are developers to blame for costly errors like the spate of IDOR attacks compromising large enterprises, like the 2019 incident affecting First American Financial Corp.? Absolutely not. Organizations will not see meaningful change until developers are incentivized to care and security programs **can effectively measure their security skills baseline** to prescribe the correct learning pathways to defend their codebase successfully.

Security maturity must go beyond dependency on tooling and AppSec-side experts. It must include deliberate measures to train and harness the power of security-skilled developers.

How do companies start with a security initiative and ultimately move to Secure-by-Design through an upskilling program?

Traditionally, companies start a security initiative when they find a significant security problem. To investigate further and understand the full spectrum of issues, they scan their applications with static and dynamic analysis tools, inevitably discovering more of these same bugs. Once that baseline is in place, they start with bug bounties to uncover and remediate hard-to-find, exploitable issues that can lead to data breaches and disruption of service.

Often, years into the program, organizations realize that they are finding issues but not necessarily fixing them long-term and that, overall, their security posture has not necessarily improved over this time period. This exacerbates the consequences of growing cyber threat where 60% of companies have experienced a breach in the past two years. There is a more effective and durable way forward.

Developers need to be enabled - through continuous, precision learning pathways and tools that suit their tech stack - to share the responsibility for security. They cannot implement what they have not been taught, and too often, on-the-job training fails to set them up for security success in their day jobs. Secure-by-Design initiatives demand that software vendors ship their products free of security bugs, and it is developers who will ultimately need to overcome poor coding patterns and insecure design principles to produce a better outcome.

Verticals by the numbers: How many developers are touching code?

Based on more than nine years of data collected from global enterprise customers, Secure Code Warrior has unique insight into organizations that are essentially a few steps ahead of others in their developer upskilling and, subsequently, Secure-by-Design initiatives.

The majority of companies on the SCW platform are in the financial services and information technology sectors. In fact, **of all companies on the SCW platform, 57% exist in one of those two categories**. This likely correlates to the above average maturity and the high level of regulation experienced in those sectors, with compliance measures like PCI-DSS a determining factor in ensuring developers have verified security skills to properly configure sensitive databases, payment gateways, and portals.

The financial services sector has the most developers currently undertaking a Secure-by-Design initiative in some form. While the average may not be significantly better, we can determine:

- **Three developers out of five are in the financial services sector;**
- **One out of five is in the information technology sector, and;**
- **One out of five developers are in all other industries combined.**

From a company perspective, 57% come from the Financial Services and Information Technology Sectors, while four out of five developers come from these Sectors. That means that the largest enterprises in terms of developers are located in those two industries.

The financial services and technology sectors are definitely thinking about Secure-by-Design initiatives. However, as a wider industry, our progress is far too slow. For example, the OWASP Top 10 has barely changed over the last two decades, and this is a consequence of us—as a wider group of security professionals—failing to eradicate an entire category of vulnerabilities in the same timeframe.

The Benefits of Benchmarking Security Skills for Developers

In recent years, speed has been the essence of software development, with developers under pressure to produce new applications, services, or updates as quickly as possible. Emerging technologies like AI coding, which developers have found helpful, have accelerated those processes.

However, increased speed and production, which can inevitably lead to deploying buggy and insecure software, only underscores the importance of following security best practices during development. These need to be applied right from the beginning of the development cycle. Software developers are clearly in the best position to ensure that coding mistakes are avoided or caught early, however, the problem is that most of them don't have the precise skills or tools to ensure that they are always producing secure code.

Providing them with the skills makes a significant and measurable difference. Developers trained in writing secure code have been very effective at reducing vulnerabilities in software. That not only reduces risk but—acknowledging that speed is a factor that won't go away—it's also time- and cost-effective. The National Institute of Standards and Technology points out that, compared with securing software at the beginning of the SLDC, fixing defects during testing takes **fifteen times longer, and fixing flaws at the deployment/maintenance stage can cost thirty to one hundred times more time and effort.**

Despite the clear benefits of developer-driven security, implementing these foundations has been a challenge for many. This includes establishing a baseline of security skills, providing training, and verifying that developers have acquired those skills by measuring them against an established benchmark. But that could be changing.

Some companies are taking advantage of advancements in developer security education to benchmark the skills their developers need. They are designing education programs to not only teach those skills but also help make applying those skills a routine part of developers' work. When compared with the rest of the industry, they are seeing clear benefits in risk reduction.

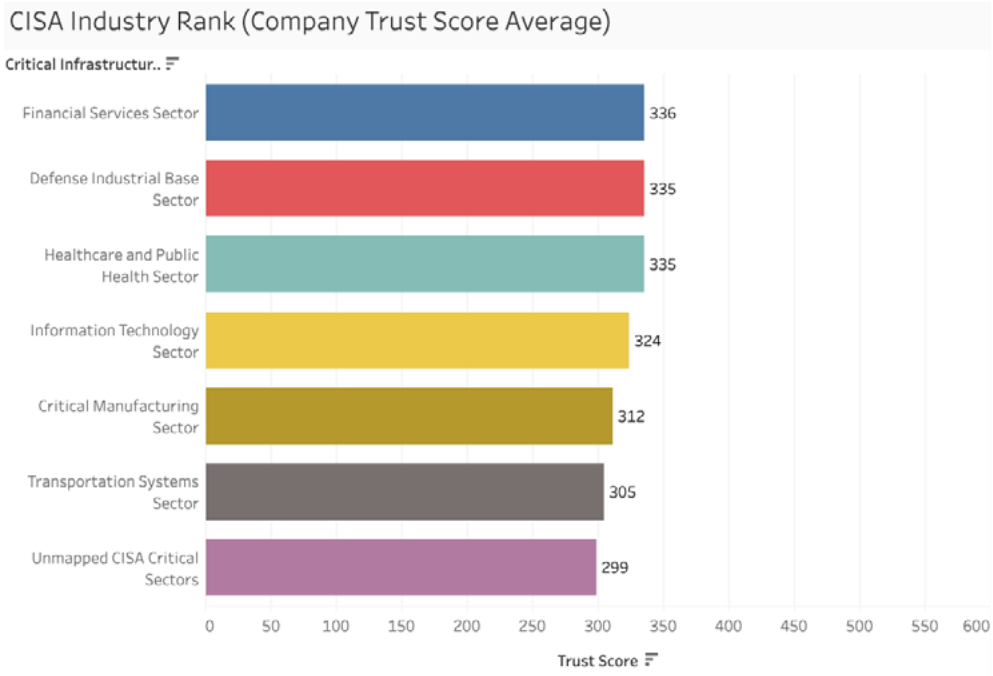
Companies are realizing that precise developer training has moved from nice-to-have to must-have, particularly with the advent of highly productive tools like generative AI coding assistants. Yes, they can help greatly boost productivity, but they can't be trusted to work unsupervised, lest they introduce errors that could spread throughout the software ecosystem.

There has been some consensus among the wider industry that, generally, enterprises in the financial services realm have the most advanced security programs, largely due to the immense compliance and governance they face. Secure Code Warrior has observed this and, anecdotally, views them as a vertical that is typically more willing to look "outside the box" for innovative approaches to training and upskilling.

But what does the data from the SCW Trust Score reveal?

Industry Secure-by-Design Initiatives as Measured by SCW Trust Score

Analyzing insights gathered from **over 20 million data points, across 600+ enterprise customers and more than 250,000 active developers,** we mapped our findings to CISA's critical infrastructure sectors to draw conclusions about cross-vertical Secure-by-Design readiness:



This chart reveals the average SCW Trust Score from a company perspective. We do *not* consider the size of the company; this is purely an average of all companies, irrespective of their size.

Compliance and regulation have always focused on banking and finance, leading to the expectation that they would be frontrunners in a comprehensive Secure-by-Design initiative. However, this does not surface from the data. **Average Secure-by-Design initiatives through upskilling (as measured by the SCW Trust Score) for each industry are very similar.** There is no one industry that dominates significantly.

When comparing the critical infrastructure sectors, some industries will be noticeably absent from our analysis. The energy and communications sectors did not meet our minimum criteria of at least 1000 developers and **at least ten companies contributing to SCW Trust Score and benchmarking data.**

In addition, **eight critical infrastructure industries are completely missing.** Those sectors heavily rely on other verticals (including the information technology sector) to develop their software or run their systems. This is a reasonable approach since, while they still have an obligation to maintain secure software and systems, they are not in the business of building their own software from scratch. This only continues to highlight the importance of CISA's Secure-by-Design Guidelines for software vendors, ensuring that end-users at least start with a Secure-by-Design product.

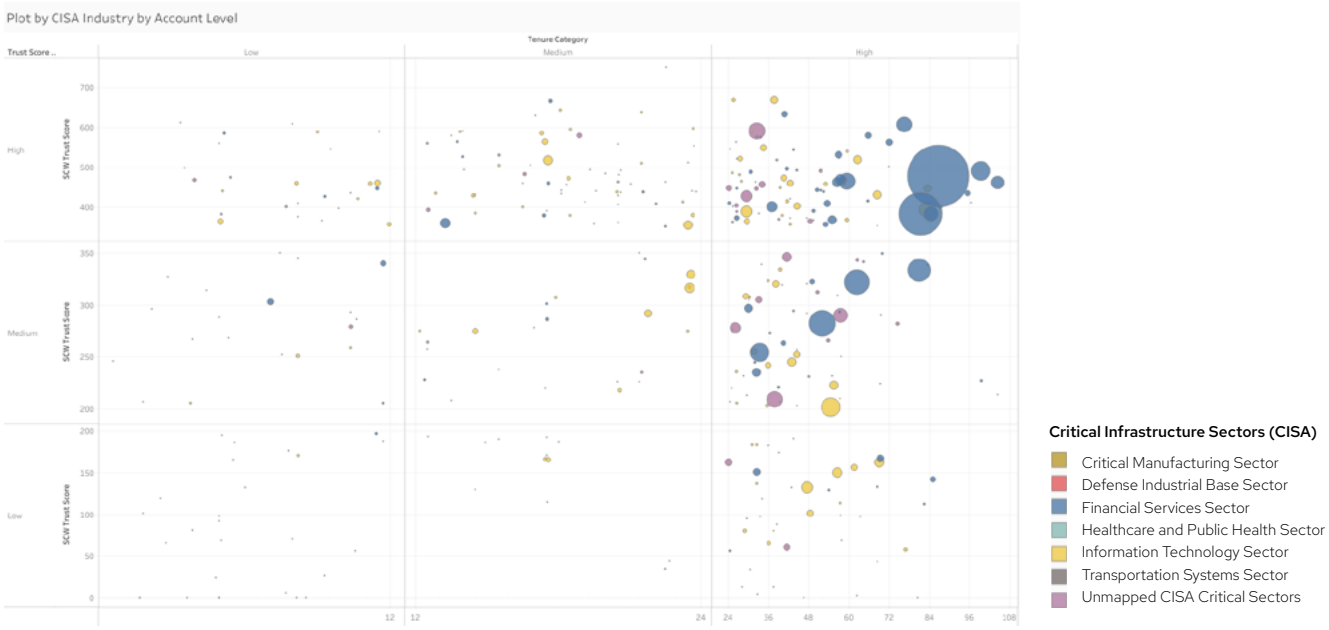
Do developer cohort numbers affect Secure-by-Design initiative success rates?

Many security leaders persistently highlight the sheer difficulty of scaling most elements of an enterprise security program, especially those involving continuous upskilling and assessment of individual personnel. This is a valid concern, but in the wake of several global legislation reforms demanding that developers have verified security skills, it must be overcome.

Our data illuminates that companies with many developers *can* be successful in a Secure-by-Design initiative. In fact, the **data shows us that most large-scale Secure-by-Design initiatives are successful, while smaller-scale initiatives are all over the map.**

Anecdotally, based on interactions with over 600 enterprise customers, we can make the educated assumption that, when a large investment is made, it becomes a company priority, and they want to succeed with the initiative. **However, the silver lining is that small companies can be successful with an initiative *quicker.***

The average SCW Trust Score of the financial services sector vertical is dragged down significantly because of small financial institutions not embracing a true Secure-by-Design program initiative:



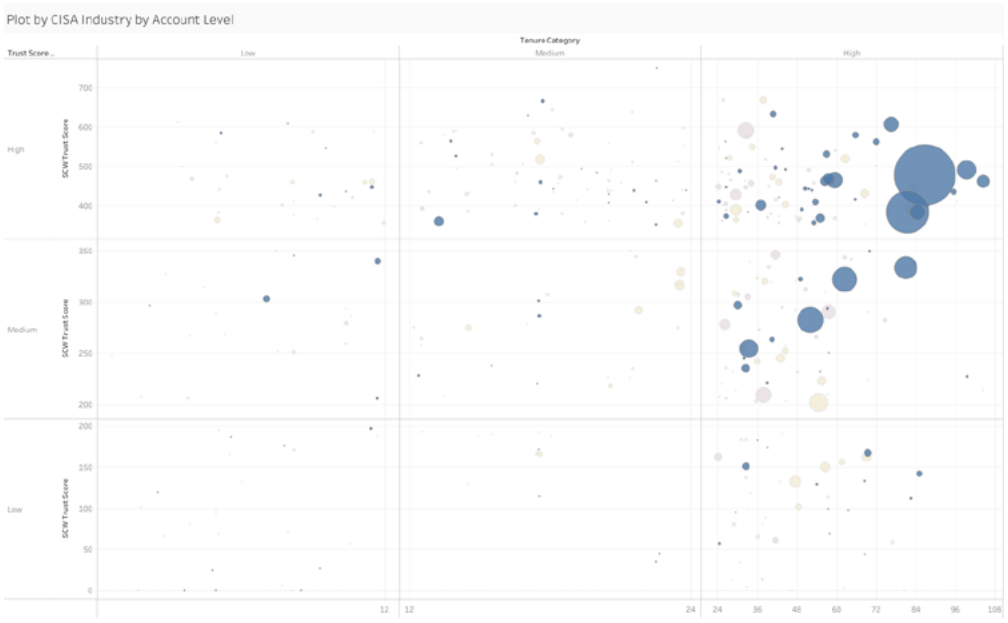
SCW Data Map

Scatter plot of individual companies in the SCW platform:

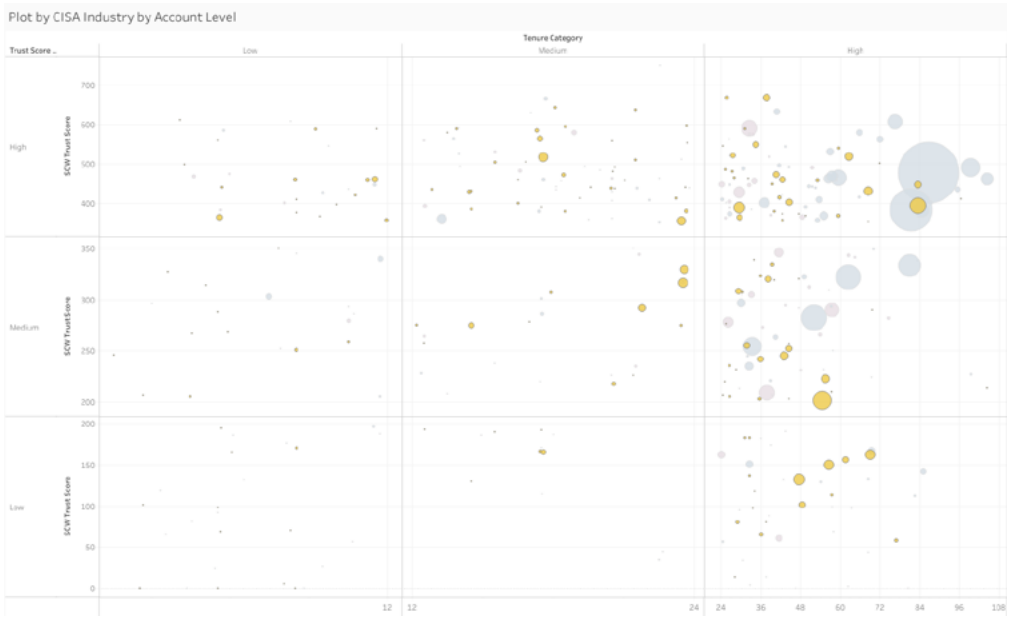
- On the horizontal axis, we see their tenure.
- The more to the right, the longer their initiative is running.
- On the vertical axis, we see the SCW Trust Score, or their level of maturity in writing secure code.
- The further to the top, the more mature.
- The bubble size relates to the number of developers in the company.
- The larger the bubble, the more developers in that company.
- The color of the bubbles represents the industry they are in.

We do see a difference in top-down vs. bottom-up initiatives. Top-down: There may be a compliance requirement. Where **large, mainly top-down initiatives in the finance sector score high, we do not see that happening in the mainly bottom-up initiatives in the technology sector,** where there is quite often no top-down mandate to implement Secure-by-Design through upskilling.

The bottom-up approach has very mixed results, as it relies on developers voluntarily taking the initiative (or not). If there is a top-down approach, you may have a better shot at succeeding with a Secure-by-Design initiative. Want to try from the bottom up? Program leaders need to understand that developers are busy, it is not their top priority, and results will vary.



Financial Services Sector



Information Technology Sector

A program of agile upskilling can resonate with developers, when it's built on established baselines, with hands-on sessions that address real-world problems that developers are facing and delivered effectively in ways that suit their already overloaded work schedules. Developers can see the advantages of improving their skills, both for the company and their own careers. It also can improve collaboration, which can help deepen the security culture within the organization and further promote ongoing improvements in safe software practices and code quality.

Reactive Vs. Preventative Security: A Hard Sell

Even in the wake of devastating data breaches punctuating every year of the past decade - from the Equifax incident, to the more recent SolarWinds supply chain attack - most security programs continue to focus on a reactive, as opposed to preventative, approach to security and general threat mitigation. While this was sufficient in decades prior, the sheer speed at which technology, software and digital connectivity are moving necessitates a decisive rethink.

Most enterprises invest in finding and fixing vulnerabilities or, indeed, incident response, as opposed to widening the scope to ensure security best practices are deployed from the start. In the context of the development cohort, this would denote that few companies are meaningfully adopting the Secure-by-Design approach of coding securely from the start, and this is reflected in our Learning Platform data. The status quo continues to uphold the notion that preventative security is a much harder "sell" than reactive measures. If we think about a similar scenario in another form of engineering, namely the car industry, this would be like investing in more paramedics and ambulances instead of working to improve automobile safety.

How did we get here? Apart from the onslaught of digital innovation making it nearly impossible for security professionals to keep pace with what is being produced and deployed, a significant number of companies—especially in the centuries-old finance sector—run enormous code monoliths, some dating back to the 1950s, when COBOL was king. Adapting to the security needs of legacy code in addition to newer applications can be immensely challenging, but a Secure-by-Design approach through upskilling is the best chance we have as an industry to right the ship.

Deep Dive: Developers Involved in a Secure-by-Design Initiative Through Upskilling

If we seek to combine the developers on the SCW platform with all of our competitors in this Secure-by-Design through the upskilling market, we have between 500,000 and 1 million developers switched on to such an initiative.

As of 2021, the total global developer count stood at an impressive 26.9 million. Projections indicate this figure will surge to 28.7 million by the end of 2024. Therefore, if we were to add the number of developers participating in an upskilling exercise to the total number of developers, it correlates to a penetration of **less than 4% of all developers on Earth who are currently involved in developer-centric Secure-by-Design upskilling initiatives.**

While this is a concerning statistic in itself, the ratio of developers to security professionals in any one company has, for many years, existed at far below optimum levels.

Referencing the large-scale BSIMM14 study of enterprise companies that are actively engaged in software security, one data point reveals that the average number of application security (AppSec) specialists per developer - or, essentially, the number of trained personnel responsible for ensuring developers write secure code - **is on average 3.87 AppSec professionals per 100 developers.** With less than four trained specialists responsible for the security of the code that is written day in, day out, by 100 developers, it is little wonder that code-level vulnerabilities continue to trip us up in increasingly potent ways.

Secure-by-Design Initiatives vs. Other Security Industries: Is it Underrepresented?

If we look at the market opportunities of other security industries, we can see the following:

- The application security market size was valued at USD 5.28 billion in 2022, and is poised to grow from USD 6.08 Billion in 2023 to USD 17.51 Billion by 2031;
- The global network security market size was valued at USD 23.83 billion in 2023, and is projected to grow from USD 26.57 billion in 2024 to USD 67.33 billion by 2032;
- The global operational technology security market was valued at USD 15.60 billion in 2022, and is poised to grow from USD 18.03 billion in 2023 to USD 57.51 billion by 2031.

It is clear that, while technically a branch of the application security market, components that drive Secure-by-Design strategy and performance are underrepresented across the board. After all, if applications were hardened, there would be no need to build "walls" around them in the form of AppSec tooling and real-time monitoring.

The Proof Is in the Trust Score: The ROI of Secure-by-Design Initiatives

Baselines and benchmarks can greatly optimize an organization's security posture by making secure coding an essential part of its DNA. However, for this to work, you have to know that the training has been effective and that developers have absorbed security best practices into their work habits. You must have complete faith that they have truly earned their license to code.

Secure Code Warrior's Trust Score allows you to track developers' progress as they work. You can gauge their progress against internal standards tailored to your organization's needs and the performance of peers and competitors across the industry.

As an industry-first solution, SCW Trust Score uses a dynamic algorithm that draws on more than 20 million learning data points culled from work at over 600 customers by more than 250,000 learners. That data set provides a baseline for a security education program and the means to assess its performance by evaluating developers' actual work.

The ROI of precision measurement and performance

Recently, we analyzed vulnerability reduction data as a result of an upskilling program for **26% of all developers on the SCW platform.** As this data does not live on the platform itself, we rely on our customers to work with us and combine data from various sources to perform this analysis. While we make ourselves available to assist, these are customer-driven computations following their own internal scrutiny of the effectiveness of SCW's platform in their organization, and the figures are reported to us. We do not have control over or input into the final result.

To measure vulnerability reduction, the average term for collecting data is one year. There are various exercises that can be enacted; the most common ones are:

- **Scan-Train-Scan:** This is where an analysis is made over a year if fewer vulnerabilities are found in the code;
- **Monitoring:** Monitor the performance of a trained group of developers compared to an untrained group of developers and their introduction of new vulnerabilities.

However, the infrastructure to measure the results of a Secure-by-Design initiative is not widely deployed today, and this factor is certain to inhibit new growth and investment in this area.

Evidence and conclusion:

If we look at our largest initiatives, we see a direct and consequential correlation between a Secure-by-Design initiative and reducing vulnerabilities. In one case study, conducted in a company with more than **10,000 developers,** we saw a **53% reduction in vulnerabilities** introduced by trained software development personnel. Interestingly enough, this company did not present as having the highest score on the benchmark, nor are they a top performer in the platform. They are statistically average.

If we focus on large initiatives (7000+ developers in a single company), they can predictably reduce vulnerabilities by 47-53%.

If we observe all the vulnerability reduction exercises we've done across our customer base, then we cover 26% of all the developers on the SCW platform. **In all the case studies combined, there is a reduction of vulnerabilities introduced by 22-84%.** We see a wider range when we talk about companies with a smaller group of developers. We also see a higher percentage of results when it is a focused training group; they zero in on a specific group of vulnerabilities with specific training, resulting in a better overall percentage.

Aggregating data on the performance of individual developers as they train and use the Secure Code Warrior platform provides clear visibility into an organization's security program and calculates an organizational Trust Score. A Trust Score not only gives you a picture of the organization's security posture, it also helps ensure that you're staying in compliance with the full slate of applicable regulations, from GDPR and the California Consumer Privacy Act (CCPA) to the Payment Card Industry Data Security Standard (PCI DSS) and CISA recommendations.

Trust Score also allows for drilling down to specific areas within an organization. Reports can be filtered according to languages, teams, or categories, producing customized reports that allow companies to address the specific needs of developers or teams and identify the areas where additional training or coaching is needed. After all, security is a never-ending endeavor; effectively benchmarking performance will help identify opportunities for continuous improvement.

All of that underscores the reality of effective cybersecurity in today's fast-moving, cloud-based, and highly distributed environments. Effective security requires that organizations build a security culture throughout the enterprise. A culture of security among developers with the training to code securely—and to have it become so much of a habit that they can do it at speed—is a good place to start.

Accelerated software development and deployment, coupled with an ever-more-menacing cyber threat landscape and increasingly hawk-eyed regulators, have put cybersecurity on the front burner. Organizations, if they haven't already, need to give priority to developing an enterprise-wide security-first culture. And because the most serious cyber threats involve data that exists in software, cultural change needs to begin with secure software code.

Developers and AppSec professionals need the training to ensure that security best practices are followed at the beginning—with the generation of code—and throughout the software development lifecycle. Just as important, however, is demonstrating that the training has been effective, and that practitioners have absorbed the lessons of creating secure code and detecting flaws in code generated by AI or other sources.

The industry needs a robust benchmark defining the skills developers should have. Companies should establish the baseline skills developers need to make secure coding a routine part of their work, identifying where skills are lacking, and providing hands-on, agile training as part of an ongoing program focused on continuous improvement. The key is being able to assess whether developers have acquired the necessary skills with a solution like Trust Score, ensuring that they can be granted access to the most sensitive areas while keeping those who aren't yet ready away from critical projects.

Proving that secure coding is the foundation of a company's software applications and services can reduce risk levels, cut the costs of remediating flaws after the fact, and lessen the chances of a major breach. It can also help convince top-level executives of the value of investing in security while ensuring that the company stays within the good graces of regulators.