SECURITY JOURNEY

JANUARY 2024

A Study on Secure Coding Training

Is Regulation the Consequence of Complacency in Securing Code?

Introduction

2023 was a year of software security regulation and governance from:

- The White House
- Cybersecurity and Infrastructure Security Agency (CISA)
- The U.S. Securities and Exchange Commission (SEC)
- Payment Card Industry Security Standards Council

We also saw the first time the SEC has personally charged a CISO for cybersecurity-related misconduct, even though they seemingly followed industry protocol.

In 2024, we expect cybersecurity regulations to become even more stringent as they remain a key focus area for industry organizations and governing bodies.

An AppSec Dilemma

Even though vulnerabilities are on the rise, **organizations** are increasing their focus on speed-to-market – the AppSec Dilemma is the challenge of balancing the need for secure applications with the need to develop and deploy applications quickly.

Notice the use of the word 'organizations' and not individuals. Many individuals acknowledge this AppSec Dilemma, but when organizations lack a strong security culture across teams and fail to keep security in mind when making business decisions, are we asking for stricter regulations with financial penalties, like GDPR?

The Study

This study of 621 IT/IT Security Professionals took place in the Fall of 2023 and was conducted independently by Ponemon Institute and is sponsored and published by Security Journey. The goal of the research was to understand the state of secure coding training and provide insights into how organizations are attempting to improve software security.

This is what we learned.

A Study on Secure Coding Training

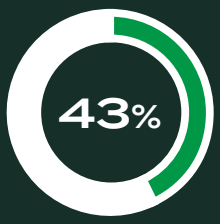
Is the failure of organizations to create security-savvy development teams due to inadequate investment of time and money?

of study respondents are only doing secure code training because of a compliance need or an exploit

These organizations are not focused on building a secure culture or educating their team on handling a broader landscape of threats, and their approach will ultimately lead to a reactive security program.

of respondents, either partially or fully, rely on in-house secure coding training

Asking already over-extended AppSec and DevSecOps teams to be not only security experts but educators as well can contribute to weakened security programs, ill-prepared teams, and position turnover.



Use a 3rd-party for secure coding training

Less than half have invested any money in expertly training their organization to secure code.

These statistics are concerning, as they indicate that organizations rely too heavily on security tools and overburden their security workforce.

Even the best SAST, DAST, SCA, or GenAI tools can help identify security issues; they should not be relied on for securing a system. These tools act as a safety net, but **it's essential to have experts who can vet the outputs from these tools and take the right actions to ensure the system's security.**

Security workforce shortages are well documented; it's predicted that millions of security professionals are needed **to fill the worldwide shortage.** Overworking an already stretched-thin security employee will inflame an already reactive security program.

How You Train Matters

When training is focused solely on meeting compliance standards, it often leads to a situation where the minimum requirements are met. Still, it does not necessarily translate into the development of expertise.

Let's take a look at some more data from the survey.

Only **36% of organizations** have their developers learn to write secure code

A mere **21% educated their developers** on vulnerability remediation

Less than half teach secure software design

61% do not deliver training in small consumable units that are well known to provide a better learning experience for adult learners.

Over **50% said that the training is not customized** to their needs

50% have no form of assessment to measure knowledge gain

68% of lessons lack immediate specific feedback, hindering knowledge retention

48% only train annually, bi-annually, or when an incident occurs

These statistics reveal a concerning level of complacency in how organizations are approaching security training for their development teams. Checking the box for compliance is easy, but organizations need to focus on more than just compliance.

They need to achieve short-term compliance goals while supporting a proactive, long-term approach to engage learners and build a more secure culture around application security.

Divides Between Development, Security, and Compliance

Only 55% of those surveyed felt their development, security, and compliance teams were aligned on product security. This implies that a significant proportion of organizations are facing challenges in achieving a cohesive and unified approach toward ensuring the security and compliance of their products.

The lack of alignment between these teams can lead to a fragmented approach toward addressing security concerns, potentially resulting in increased security risks and vulnerabilities.

51%

blamed silo and turf issues for significant delays in vulnerability patching

33%

said there is not a common view of applications and assets across security and IT teams

38%

said they don't have the ability to hold other departments accountable for patching

The lack of shared focus and accountability can lead to major delays in vulnerability patching, which can be a significant risk to businesses. There's still more work to be done to break down silos and improve collaboration between teams to ensure that they can effectively manage security risks.

The Vulnerability Patching Crisis

Organizations are struggling to remediate vulnerabilities in their applications effectively. From proper detection to effective remediation, organizations are experiencing what happens when relying solely on tools to catch vulnerabilities before they are released to production – and this is a widespread problem.

According to a study conducted by Qualys, 25% of vulnerabilities were exploited on the day of their publication, and 75% of vulnerabilities were exploited within 19 days (approximately three weeks) of publication. This indicates that securing an application later in its development lifecycle is a risky plan, as it leaves it vulnerable to immediate exploitation. Knowledgeable human intervention can improve this situation.

Vulnerability Patching Study Results

- **Over 60% of organizations believe** it is difficult to very difficult to remediate vulnerabilities in applications
- **Only 11% of organizations believe** they patch vulnerabilities effectively in a timely manner
- **47% said lack of qualified personnel** makes it difficult to remediate vulnerabilities in production

In addition to these problems, only 20% of organizations are confident in their ability to detect a vulnerability before it is released. And only 50% of organizations test the security of their applications after they have been released. Once again, this signals that too many organizations have given up the fight.

In the past year, **54% of respondents had a security incident** due to an unpatched vulnerability with **51% having more than 8 security incidents** because of an unpatched vulnerability.

Will new compliance regulations prompt organizations to prioritize vulnerability management to avoid reporting material incidents to the SEC?

As this report is being written, the SEC's New Cybersecurity Disclosure Rule has officially gone into effect, and on the very first day, VF Corporation, a global brand recognized for brands like The North Face and Vans, reported a significant cyberattack to the SEC.

Compliance Requirements that Focus on Software Security

The question posed at the beginning of this report is, Is regulation the consequence of complacency? Here's a recap of the regulations and their focus on software security to shine a light on the most recent regulatory focus.

Cybersecurity and Infrastructure Security Agency (CISA)'s Secure By Design Guidance

The 2023 CISA Secure by Design Guidance emphasizes the need to prioritize security from the very beginning when building products that rely on technology. It states that the current reactive approach to cybersecurity is proving to be inadequate and suggests a shift in responsibility for security from users to manufacturers and developers. This will help to build products with better resilience against cyber threats.

The White House National Cybersecurity Strategy

The National Cybersecurity Strategy proposed by the White House suggests that software manufacturers should be held accountable for vulnerabilities in their products. This includes limiting the use of EULAs and modifications to product liability laws. Manufacturers who release software with known security flaws or fail to patch them promptly may face financial penalties.

The U.S. Securities and Exchange Commission (SEC) New Disclosure Rules

The SEC has recently introduced a new regulation that makes both organizations and individuals within the organization accountable for cybersecurity incidents. Public companies are now mandated to disclose any significant cyber incidents they encounter, along with their comprehensive strategy to manage cyber risks.

Payment Card Industry Security Standards Council

PCI DSS v4.0 highlights the importance of maintaining security as an ongoing process. One of the key changes introduced in this version is the requirement for organizations to create detailed documentation of their efforts in secure coding training and following secure coding approaches. This documentation is critical in demonstrating compliance during audits and assessments.

It becomes clear that each of these governing bodies has a keen eye on insecure software and are providing specific guidance and requirements to change that. The advantages outweigh the hurdles. It's important to remember that it's not just about patching vulnerabilities after the fact but about prioritizing security from the beginning.

Conclusion

This Study on Secure Coding Training revealed what so many security professionals live and breathe daily: that organizations prioritize speed to market over security. While government and regulatory agencies have been patient and attempted to let commercial businesses handle software security in their own way, that era appears to be ending.

The increased pressure from government and regulatory bodies should feel like a call to action for organizations to empower their critical security and development resources to work together on prioritizing security.

Education can be the starting point for cultural change, removing complacency so that both security experts and development teams have a shared focus on securing software from the start, preventing regulations from growing to include stricter definitions and financial penalties.

> “The great aim of education is not knowledge, but action.”
>
> **- Herbert Spencer,** Philosopher

About Security Journey

Security Journey is a leading secure coding training provider with a mission to help organizations educate development teams to build secure software and reduce organizational risk.

You can learn more about this study and other application security topics at: securityjourney.com/resources.