

[Schedule a Demo](#)[← Back To Security Journey Blog](#)

# Beyond Security Awareness: Safer Apps through Education



# Beyond Security

Oct. 7, 2022

## Awareness: Safer Apps through Education

---

The past decade has seen security awareness go from a new concept to a security strategy embedded in most organizations. Several regulations recommend security training but do so in very broad terms.

Most organizations choose security awareness programs to meet these recommendations. And this approach is effective for most employees. These programs deliver communications, training, and motivation across the board. No matter the role, employees have access to the information they need to stay informed about the latest cybersecurity threats, like social engineering attacks.

But is awareness enough for security-critical roles, like software developers? While compliance regulations like PCI do call for secure coding training, there is little guidance about how to satisfy this requirement. Many organizations offer developers video or computer-based training that covers the basics of the latest OWASP Top 10, then call it a day.

At best, these efforts to meet the minimum secure coding training compliance requirements result in a “tick the box” exercise. Developers watch the video or complete the module, mark their “training” complete, and wait to repeat the exercise again next year.

While this approach is right for the level of security knowledge needed by general employees, the people who build the software need deeper education on application security practices. Without it, software engineers and developers end up writing less secure code which introduces vulnerabilities.

And what about all the other roles in the software development lifecycle (SDLC)? From product and UX managers to QA and scrum masters, the people responsible for delivering safe applications need training that goes beyond a “check the box” approach. As the saying goes, “you don’t know what you don’t know,” and that is especially true with non-developer roles in the SDLC.

Without proper training, product managers don’t know how to prioritize security-enhancing features. QA folks aren’t aware of the best ways to test for security issues. DevOps doesn’t understand the impact of including the correct tools into the build pipeline to lower production vulnerabilities or even which tools to incorporate.

As Professor Jason I. Hong from the School of Computer Science at Carnegie Mellon University noted in a recent roundtable discussion, *“Compliance regulations are generally a good thing, but they need to move beyond being procedurally oriented, like the tick the box approach we have now, and instead focus on measurable outcomes to be effective.”*

# Security Awareness v. Security Education for Security-Critical Roles

*So, what is an organization to do?*

To build safer applications, organizations must move beyond awareness and begin educating security-critical roles. The results of this education must be measurable, too.

The first step to any successful education program is understanding the difference between awareness and education as it relates to security-critical roles.

## Security Awareness

The goal of any security awareness program is to teach users how to recognize common security threats. Upon completion, users understand the basics of cybersecurity threats against the organization. For many roles, this type of training is enough. But not for security-critical roles, like developers.

Developers often refer to the act of recognizing threats as “code smell” – the ability to identify something in source code that indicates a bigger, underlying issue. But recognition is often where things hit a wall.

Developers can recognize threats but often lack insight into how to fix – or, better yet, avoid – common application security risks. They might master code smell, but they do not know how to resolve it.

Chances are developers have not had the necessary education to solve the risks they identify. A [recent Forrester report](#) notes that none of the top 50 colleges and universities even require courses in secure coding or secure application design in their computer science programs.

Organizations that build software are obligated to fill this knowledge gap with security education for everyone involved in software creation.

## Security Education

Good security education programs teach developers the necessary skills to problem-solve security threats. The best security education programs teach development teams theory, then ensure that developers develop the necessary skills to proactively secure applications during the development phase.

When developers have both knowledge and skills, they can scale to new environments and manage unfamiliar problems. This is a valuable ability since the threat landscape is always evolving. The vulnerabilities of today will not be the vulnerabilities of tomorrow.

As John Campbell, Director of Content Engineering at Security Journey, advises, *“Good security education takes developers beyond code smell and empowers them to fix problems and, even better, code to avoid those problems in the first place.”*

Ready to follow John’s advice and move beyond awareness to build more secure applications through proven application security education? Check out our recent webinar on [How to Start an Effective Secure Coding Training Program](#), and get started today!



**SECURITY JOURNEY**

## Cybersecurity Education vs. Awareness Report

Where does cybersecurity awareness stop and cybersecurity education start?

[Download the Report](#)

The banner features the Security Journey logo on the left. The main text asks where cybersecurity awareness stops and education starts. A dark button with white text says 'Download the Report'. On the right, there is an image of a man in a blue shirt looking at a computer monitor displaying code. Behind him is a document titled 'Education vs. Awareness' with the subtitle 'Why a Programmatic Approach to Secure Coding Training Matters'.

[← PREVIOUS POST](#)

[NEXT POST →](#)

Stay Up-to-Date on all Security Journey news and events.

First name

Business Email\*

[Subscribe](#)