WHITEPAPER

Unblocking the Path to AppSec Training Success

Security Compass

To remain competitive and compliant from both a regulatory and customer demand perspective, companies of all sizes need to train developers and engineers at scale in secure development and implementation. While finding training material is far simpler than it was years ago, many organizations still struggle with managing effective programs.

It should not be this way. Quality course material is available, e-learning platforms are simple to acquire, and development personnel are eager to improve their skills. However, we often see organizations stumble over common obstacles that inhibit their ability to deliver and support training. These include:

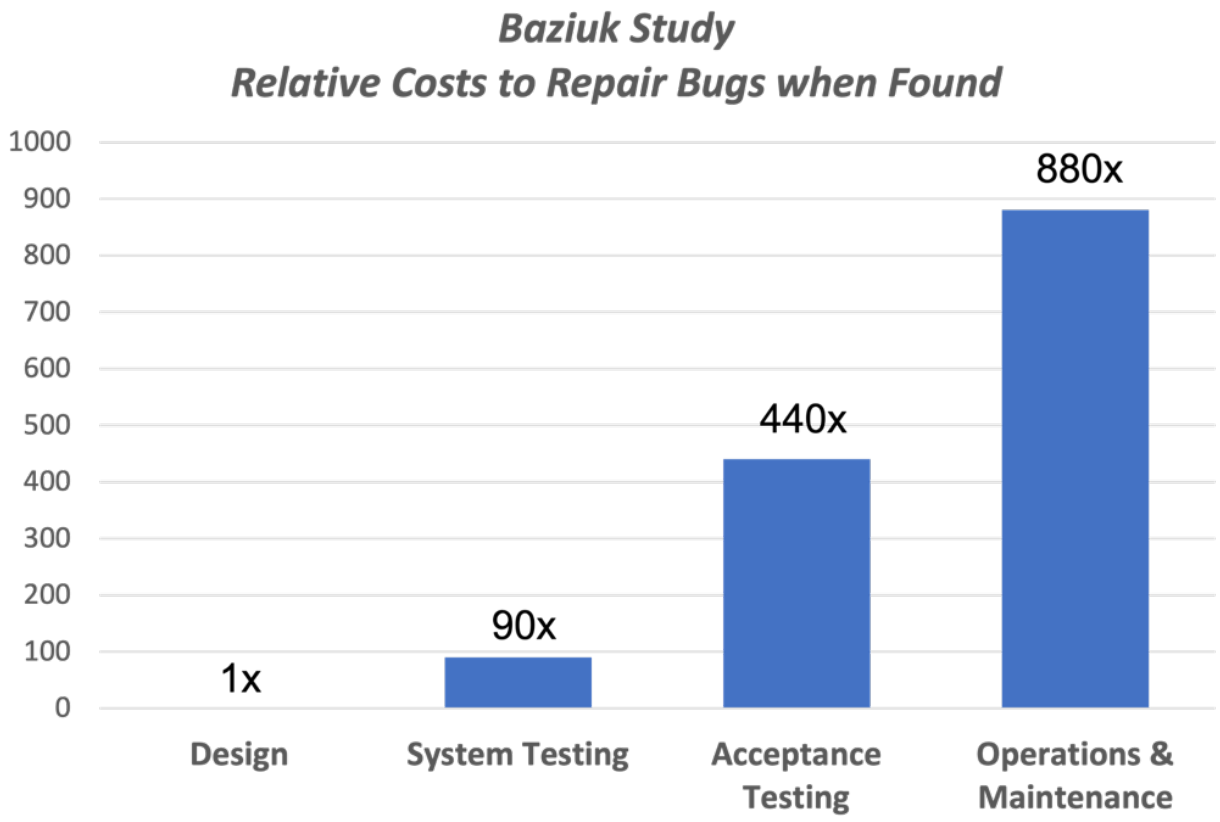
1. Event-focused v. process-focused training
2. Training by mandate v. career development
3. Withholding accreditation
4. "Comprehensive" v. targeted training
5. Relying on AppSec training alone to create a security culture

This paper will review these challenges and provide advice on how to avoid traps that can sabotage a team's efforts to succeed with educating their teams and building a strong security culture.

Why AppSec Training?

Design and coding errors in software can result in vulnerabilities. In a best-case scenario, these are found during security testing and merely delay releases and increase costs. In a worst-case scenario an adversary exploits the weakness that may have resulted from a lack of knowledge to defend and secure the code. The resulting breach can result in financial, regulatory, and reputational damage.

Training can help developers avoid costly errors, saving time and effort, and boosting your security program. One study found that it can cost hundreds of times more to fix a bug found after software is released compared to preventing those bugs from entering the code base during the requirements and design phases (thank you threat modeling). Finding and fixing those errors during the coding phase reduces remediation costs by over 90 percent.



Challenges in AppSec Training

Today's environment demands more secure software. Attacks are increasing and customers, including the US federal government, want to secure their supply chains. Regulations like the Payment Card Industry Data Security Standard require annual training on secure software design and secure coding principles. Simultaneously, market pressures require shorter development cycles. Developers can struggle to keep up to date with new languages and frameworks used in their technology stack. Staying current with evolving regulatory requirements and secure coding standards often takes a back seat.

Unfortunately, universities do not address secure coding in their undergraduate programs. An article in the Harvard Business Review noted that only one of the US's top 24 undergraduate programs require security coursework as a core requirement. That leaves it in the hands of employers to teach secure coding. In short, having a successful AppSec training program is no longer an option.

5 Security Training Obstacles to Overcome

Whether you are starting a new AppSec training program or looking to mature an existing one, there are five common security training obstacles to overcome. Here's how you can unblock your path to training success:

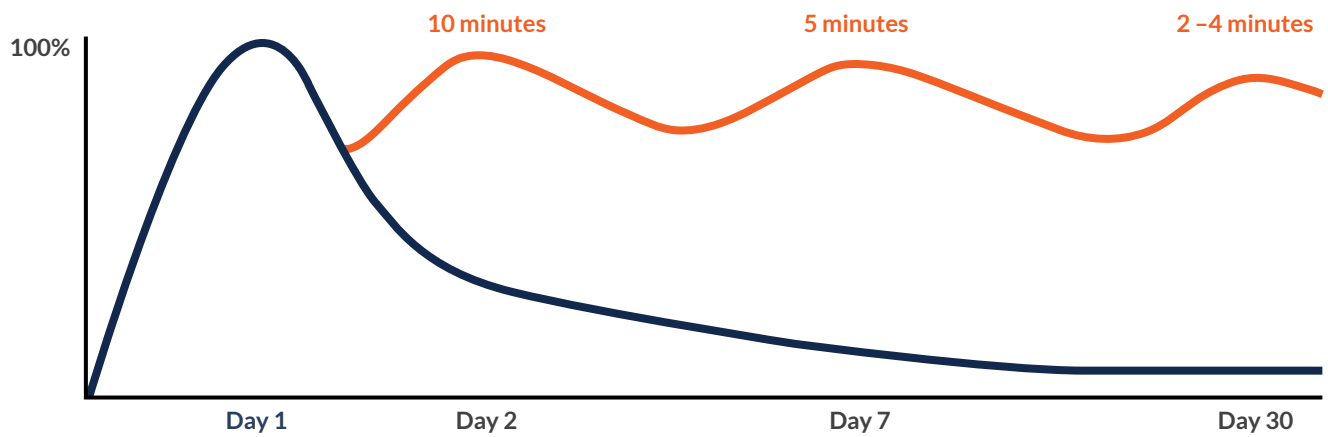
1. Event-focused Training

Many organizations meet compliance requirements through annual events. These can be as simple as reading and acknowledging your corporate information security standards or taking an "Introduction to Security" eLearning course. The long-term success of these, to nobody's surprise, is minimal. You do not learn to drive a car by attending a drivers' education seminar or become fluent in a new language by listening to a single language learning lesson. Similarly, you do not retain security knowledge without repetition over time. Limiting training to annual events also means that teams will constantly lag behind understanding emerging threats.

Successful training programs recognize that learning is a process, not an event. This has been studied and proven many times. The graph below from the University of Waterloo is representative. People begin to forget information learned immediately after a lesson. By the end of a week, a typical student can recall only 10 – 20 percent of the information from a lesson. Repetition reduces knowledge loss. The orange line in the graph represents reduced "forgetting" when the information is reinforced (reviewed) for short periods over the first 30 days. Now, instead of retaining 10 percent of the information from the lesson, the student retains 80 – 90 percent.

What you can do

Make AppSec training part of your DevSecOps environment. If a developer needs information on secure coding topics like input validation, they should not need to sit through a three-hour lesson. Small, on-demand, targeted lessons can complement more comprehensive lessons.



2. Training by mandate v. career growth

Training for secure coding is a requirement for the PCI DSS and recommended in other regulatory standards. Organizations that treat training as a chore rather than a benefit will not realize the full value of the program.

Training mandates from security increase friction between teams. Edicts deliver a message that – without the threat of penalties – development would not consider security a crucial factor in the development process. This positions training as a "stick" instead of a "carrot."

This ignores the fact that software engineers want to improve their skills – including the ability to develop more secure code. A better approach is to position AppSec training as a benefit and a way for developers to take command of their own career growth. Provide the ability to take extra courses and explore new topics. This is backed by research. One study found that 92 percent of employees say that training programs positively affect their level of engagement.

What you can do

Make sure your teams understand that the organization views its training program as an investment in its employees rather than simply a compliance mandate. Make your entire course catalog available. Beyond the one or two courses required by regulators, having more material available and reference-able will reinforce for your team that you're invested in their learning and growth.

3. Withholding accreditation

In ISACA's State of Cybersecurity 2022 report, 82 percent of the participating organizations predicted an increase in demand for technical cybersecurity positions. This means an individual trained in AppSec has more career opportunities than an untrained individual. While a worker can add internal training courses to their CV, completing an independent accreditation program is better. Learners appreciate them as they are "portable." Some employers dislike them because they fear it will make it more difficult to retain employees.

However, this position is short sighted and can backfire. Customers like accreditation programs as they demonstrate an organization's commitment to security. In an industry increasingly concerned with the security of their software supply chain, this can provide organizations with a competitive advantage.

It is important for organizations to switch their thinking on accreditation. Instead of worrying that a developer may leave because they have accreditation, think about accreditation as a retention strategy. 87 percent of millennials believe "professional or career growth and development opportunities" are important to them. Another found that "94% of employees would stay at a company longer if their training and development were invested in."

What you can do

A company-supported accreditation program is an employee benefit. There are many certifications and accreditations individuals and organizations can consider, including accreditations from bodies such as (ISC)2, GIAC, CompTIA or ISACA.

4. "Comprehensive" v. targeted training

While some companies provide very narrow training, others can go too far in the other direction. What starts as a simple program is amended from year to year, adding new training requirements on top of existing ones. For example, a developer may be part of a team building software subject to a particular regulatory requirement or using a specific programming language. The next year, she switches to a different project but still has refresher courses assigned for her previous role. Training "creep," like "scope creep," saps efficiency from teams. Eventually, users are forced to complete lessons that have little relevance to their roles and responsibilities.

What you can do
Tailor your programs to meet the roles and needs of their employees. Instead of monolithic courses that require hours to complete, target your training to each users' areas of responsibility. In addition to technical training, remember that leadership training and awareness training are also important.

5. Relying on AppSec training alone to create a security culture

A security culture in an organization is one that prioritizes the protection of sensitive data and assets, promotes good security practices, and encourages a proactive approach to security risks and threats. A strong security culture helps protect an organization by acting as a "human firewall" against cyberattacks.

While AppSec training is a key component of creating a strong security culture, it is not the only component. Creating a security culture is a continuous process that involves a combination of education, training, communication, reinforcement, and enablement with scalable processes and usable technology. It requires the active support of senior managers – even when (or especially when) release deadlines are under pressure.

What you can do
We are strong proponents of supporting your training with advocates from security champion programs. A security champion is a person from a development background who is willing to evangelize and advocate for the cause of security. The idea is to select developers who are willing to function as subject matter experts for your security needs, thereby helping drive a security culture. Good security champions act as force multipliers, extending the reach of the scarce security resources. They model a growth mindset regarding continuous and relevant security training and will help you bear and maintain a culture of security.

How to Get Started

Training in secure coding is a necessary part of protecting your organization's assets and reputation. It is also a valuable tool for employee retention. Security Compass offers a full suite of role-based and technology-specific content optimized for any business that develops custom software.

You can learn more about our offerings here.

Security Compass

Security Compass is a leading cybersecurity company that was founded in 2004 by a team of experienced penetration testers and security professionals. With a strong commitment to developing secure applications, Security Compass has become a pioneer in the application security industry. The company's Security by Design philosophy ensures that systems are built with security in mind from the very beginning of the development process. By integrating with existing DevSecOps tools and workflows, Security Compass enables organizations to shift left and build secure applications that are protected against potential cyber threats. In addition to its security solutions, Security Compass is also a trusted provider of Application Security Training. The company offers a full suite of on-demand, role-based courses covering various programming languages, cloud solutions, and IaC tools. Security Compass aims to create a culture of secure development and help reduce cyber risks by educating individuals and organizations on best practices in application security. Security Compass is trusted by leading financial and technology organizations, the U.S. Department of Defense, government agencies, and renowned global brands across multiple industries. Its flagship product, SD Elements, is an automated, developer-centric approach to threat modeling, secure development, and compliance. It helps organizations accelerate their software time-to-market while reducing cyber risks. Security Compass is dedicated to helping organizations build secure applications and empowering individuals to do the same. For more information, please visit www.securitycompass.com

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

TORONTO OFFICE
325 Front St. West
Suite 103
Toronto, ON
M5V 2Y1

NEW JERSEY MAILBOX
8 Lombardy Street, #40201
Newark, NJ
07102-3210
USA