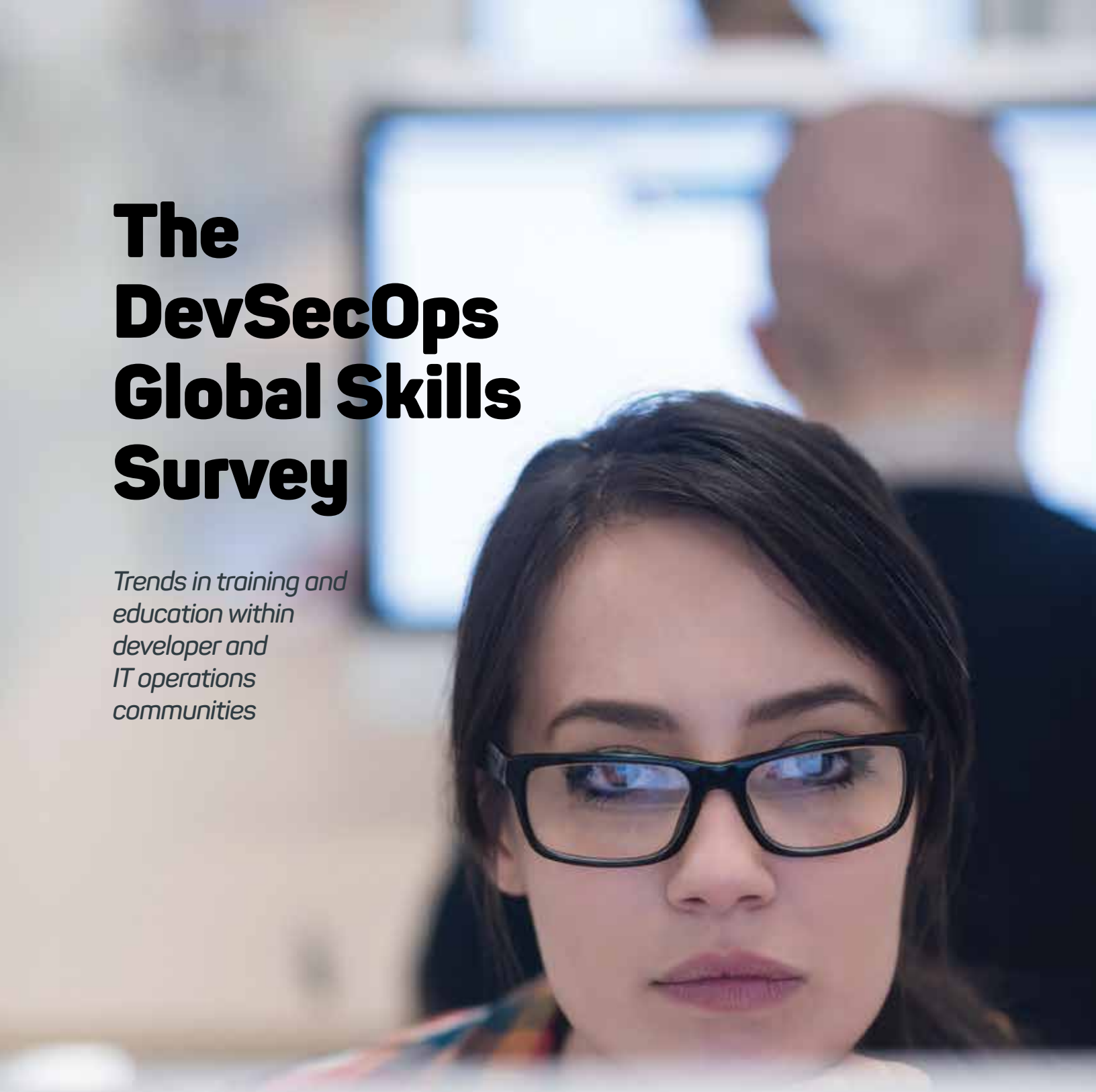


The DevSecOps Global Skills Survey

Trends in training and education within developer and IT operations communities

DevOps.com

ca technologies | VERACODE

Executive Summary

As the DevOps movement gains momentum and maturity, IT organizations increasingly struggle to fill out their IT teams with the right mix of employee skills. The challenge is twofold. The first problem is simply finding employees with the balanced combination of technical acumen and solid interpersonal skills needed to support a fast-paced and collaborative continuous delivery environment. The second is even more daunting: finding employees of that mold who also have the grounding in security principles and tooling necessary to deliver both continuously and securely. This is one of the fundamental stumbling blocks impeding IT's evolution to secure DevOps — better known as DevSecOps.

In order to understand the skills deficiencies and their causes more fully, DevOps.com recently engaged with close to 400 DevOps professionals to discuss their views of the state of today's workforce. Sponsored by Veracode, this "2017 DevSecOps Global Skills Survey" primarily focused on developers and operations experts, with a smattering of security and QA professionals in the mix. In addition, DevOps.com interviewed a number of experts in the security community at the academic, practitioner and vendor levels to gain additional insights into the nuances of DevSecOps training challenges.

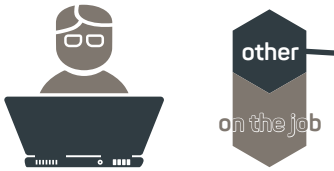
Study Highlights

Nearly 40% of organizations said the hardest employees to find are all-purpose DevOps gurus with sufficient knowledge about security testing.

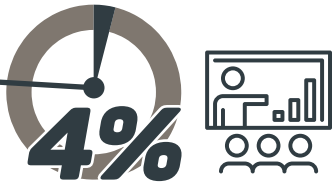
Almost seven in 10 developers said their organizations don't provide them with adequate training in security

The top two skills hardest to find in IT ops talent are vulnerability management and containerization skills.

More than 76% of college-educated respondents said they weren't required to complete any courses focused on security during higher education.



An overwhelming majority of DevOps professionals — over 64% — said they learned their most relevant skills on the job.



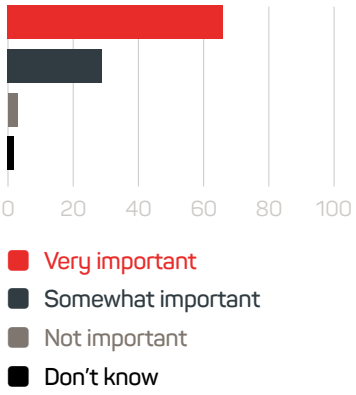
A miniscule 4% said they learned their most relevant skills from third-party training.

But more than one in three respondents said this kind of training–in the classroom or through e-learning–would be the most effective way to gain new skills.

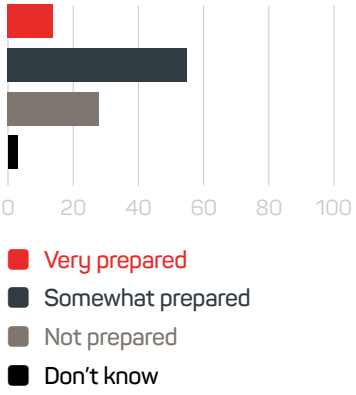
Many employers aren't stepping up the challenge — only about half of respondents said their employers paid for additional training since their entry into the workforce.

Assessing The Scarcity

How important is it to have knowledge of DevOps when entering the modern IT workforce?



Do you believe your IT workforce is prepared with the skills to securely deliver software at DevOps speeds?



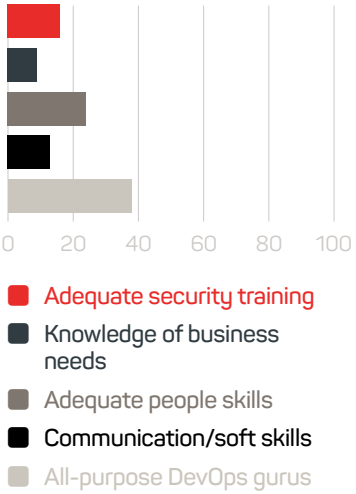
DevOps-related skills are no longer a nice-to-have feature in a job candidate's resume. Businesses today endeavor to scale their software development efforts for the app economy. They strive to move quickly to respond to constantly changing customer needs and market conditions. And they try to do it all in a secure manner.

In order to securely and continuously deliver software, organizations require a workforce with the know-how to operate in a DevOps environment with as little added risk as possible. An overwhelming majority of survey respondents said it is important to have knowledge of DevOps when entering the modern workforce, with over 65% classifying it as "very important."

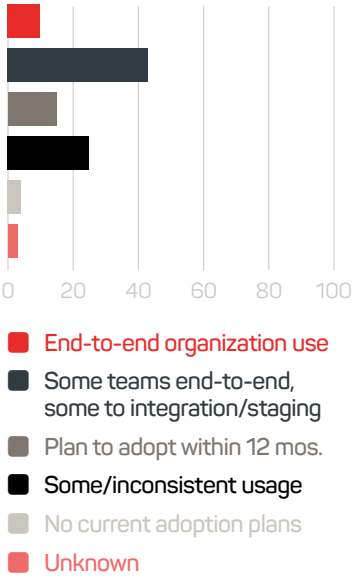
Yet organizations struggle to find the right people who fit that bill. Nearly one in three technology professionals said the IT workforce is unprepared to securely deliver software at DevOps speeds, and just over half said they believe it is only somewhat prepared.

Deficiencies in the workforce vary, with a fairly even spread of complaints that include finding developers with adequate security training, finding security people with enough understanding of the business, and finding technical staff who can play nicely with others and communicate effectively. The plurality of respondents, though, said they believe the hardest-to-find individuals are all-purpose DevOps gurus who also have a solid foundation in security testing and fundamentals.

What are the hardest skills to find to support your current DevOps/continuous delivery goals?



What is the state of DevOps adoption within your organization?



The lack of fully trained candidates could be keeping many organizations from making good on their continuous delivery ambitions. Only a small fraction of respondents — about one in 10 — can boast using DevOps practices from development to production across the entire organization. Most either employ DevOps within limited teams or inconsistently across the business. Others are just now planning to start on their own DevOps journey within the next year.

DevOps veterans well understand the principles of technical debt. It accumulates when an organization continues to choose quick-and-dirty coding or architectural shortcuts over more difficult but thorough approaches. Doing the job fast instead of doing it right means the organization will likely face expensive rework and maintenance tasks later down the road.

The statistics gathered in our survey point to a similar personnel debt that DevOps-oriented organizations face: the kind that accumulates when organizations plow forward with DevOps makeovers that don't bake training and education best practices into their transformation strategies. Organizations that fail to address these debts now will likely have to pay later with interest. Such as surcharge could come in the form of stalled-out or failed DevOps efforts, as well as heightened risks to software infrastructure that could even cause costly breaches and theft of intellectual property.

Limitations Of Classroom Learning

Do you think the security education you received is adequate for what your current position requires?

Were you required to complete any courses focused on security during higher education?

One point our survey makes clear: There are no shortcuts around DevSecOps skills shortages. Organizations will have to pony up for the scarce developers or IT pros circulating in the job market who also have security skills, or they'll need to train their own cadre. More likely, they'll need to do both.

Because if there's one sure bet, it's that new developers and IT ops folks recruited from college aren't coming out with even a whisper of the security wisdom or technical chops necessary to get the job done. The majority of our survey respondents hold Bachelor's or Master's degrees, most in computer science or IT-specific degree programs. Among those, approximately 70% said they think the security education they received was not adequate for what their current positions require.

So if you've been clinging to the hope that you can sidestep the issue by hiring fresh-from-college recruits schooled in modern DevSecOps curriculums, abandon it. Fast. A shocking three-quarters of college-educated respondents to our survey said they were never required to complete a single course focused on security during higher education.

Granted, the majority of this survey's respondents are veteran practitioners with five or more years of experience in the IT workforce. However, our interviews within the academic community indicate not much has changed in the intervening years. The academic experts we talked to explained that today's typical computer-science program still does not tune itself to the security needs of a fast-paced IT organization.

"If you actually look at the ACM curriculum guidelines for what someone with a computer-science degree is supposed to

"Most of the code that we teach people to write in basic computer classes is actually wrong. You are trying to teach them how to create a specific algorithm for doing something, and you are not really focused on the correct handling of input and output, which is where security vulnerabilities lie. This needs to be embedded in the curriculum from the beginning, instead of just waiting for somebody to teach a security class."

— Rob Olsen
Rochester Institute of Technology

come out with today, ACM mandates between three to nine lecture hours," says Rob Olsen, a professor of programming, mobile security and web app security at Rochester Institute of Technology (RIT), as well as an advocate for improving security curriculum in higher education. "That's not credit hours–that's three to nine lecture hours of security for a four-year compsci degree."

Within those guidelines, he explains, one to two lecture hours are dedicated to secure design, one to two hours to defensive programming, two optional hours to network security and one hour to threats and attacks.

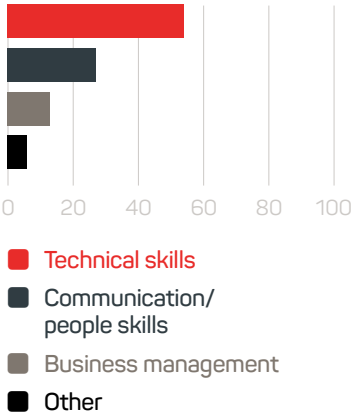
"And then this is one of my favorites: one lecture hour on all of cryptography," Olsen says. "And that's optional."

What's more, the generalized programming classes often teach future coders with examples of code that are inherently insecure, says Stefano Zanero, an information security consultant and associate professor at Politecnico di Milano. In other words, developers are learning to ply their trade insecurely from day one.

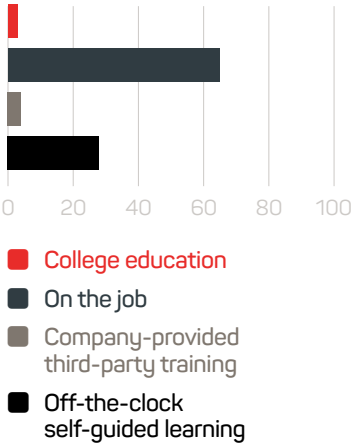
"Most of the code that we teach people to write in basic computer classes is actually wrong. You are trying to teach them how to create a specific algorithm for doing something, and you are not really focused on the correct handling of input and output, which is where security vulnerabilities lie," Zanero says. "This needs to be embedded in the curriculum from the beginning, instead of just waiting for somebody to teach a security class."

None of this means colleges have completely ignored the growing demand from the private sector for cybersecurity

What skills do you think students need to learn in college in order to thrive in DevOps environments?



Where do you think you learned your most relevant skills for your profession?



expertise in new graduates. The problem is the way they've moved to fulfill this demand might be counterproductive to the DevOps ethos of embedding security and ops into the engineering function.

"We're seeing 25% of colleges offering a dedicated computing security program at this point," says Chaim Sanders, a professor at Rochester Institute of Technology. "So that seems to be an interesting–although not necessarily effective–maneuver because it separates out who will essentially become the developers from the people who are going to be doing security in organizations. But in a modern environment, both computing security professionals and software development professionals need to be responsible for security."

In other words, the academic world is stratifying security expertise, whereas in the real world, organizations want less stratification and more IT experts with a broad base of security knowledge.

Even more troubling is the fact that even within this specialized security stratification, the curriculum doesn't serve DevSecOps because very little course work focuses on application security, Sanders says.

Clearly, it is going to take some major retooling of collegiate curriculum to meet the needs of the DevSecOps jobs marketplace. If they had their druthers, many respondents said they believe the improvements that'll properly prepare candidates should emphasize technical skills. That said, not an insignificant number think that DevOps greenhorns coming out of school might be best served with an education in communication and business management skills.

"At the university level your education is about learning to learn. As a developer you don't learn every framework and language that are popular today. You learn the fundamentals of computer science and then you learn how to learn the next thing that comes out. It should be the same with security — it's learning to learn about security."
— Michael Feiertag
CEO, tCell

Given Sanders' and Olsen's analyses of today's computer-science curriculum, it's no surprise that a measly 3% of survey respondents reported that they learned the most relevant skills for their profession through their college educations.

Rather, the majority of respondents said they learned the most important skills on the job, with self-guided learning ranking second. Now, these answers might not necessarily be a reflection of the shortcomings of college degree programs but instead be a reminder of the power of proficiency gained by experience.

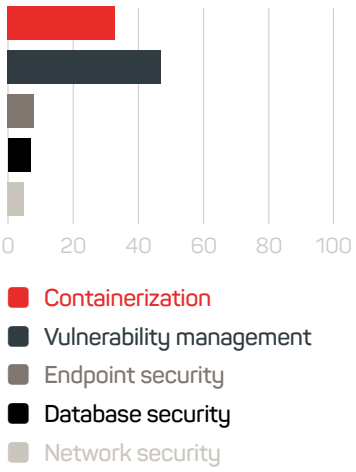
Either way, the perceived value of post-collegiate skills building by respondents can potentially offer a big hint for curriculum designers' frame of mind in bolstering the security content of existing courses.

"At the university level, your education is about learning to learn. As a developer, you don't learn every framework and language that are popular today. You learn the fundamentals of computer science, and then you learn how to learn the next thing that comes out," says Michael Feiertag, CEO of security startup tCell. "It should be the same with security–it's learning to learn about security. It should be learning to be literate, for example, in the latest methods that the bad guys are using. And if you know that, then you're likely to figure out how to counteract it, right?"

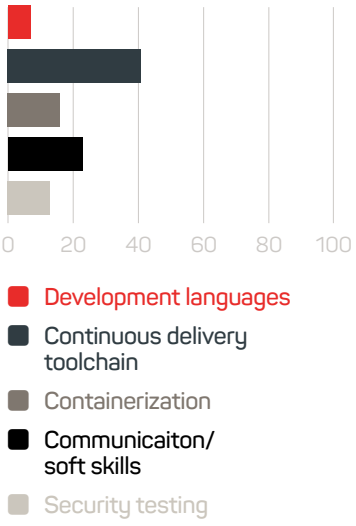
He warns universities not to further inculcate the checkbox security mindset by shoehorning in a "templated view of the world" with teachings that simply provide students with a list of items they need to review before shipping software. It has to be more fundamental than that.

State Of Continuing Education

Which security skills are hardest to find in IT ops talent?



What skills do you think the IT team most lacks in that pursuit?



Regardless of what the answers are to cure the deficiencies in collegiate curriculum, the fact of the matter is those are very long-term fixes. That is why it's going to be up to the industry and individual organizations to take some immediate short- and medium-term steps to fill in the DevSecOps skills deficits that exist today.

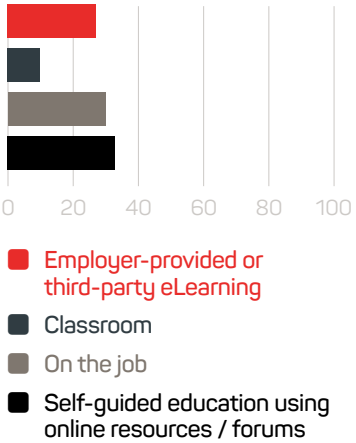
For example, ops folks complain that they're having a devil of a time finding IT talent with enough knowledge about vulnerability management and containerization.

And from a complete team perspective, over 41% of respondents reported that their teams lack the necessary knowledge and experience with the continuous delivery toolchain to help them securely deliver software at DevOps speeds.

The status quo is not working. Our survey uncovered a big disparity in the lack of formal continuing education opportunities afforded to those in the DevSecOps workforce who crave it. As we've already pointed out, only about 4% of our respondents said they learned their most relevant skills through third-party training offered by their companies. But that doesn't mean many respondents wouldn't value this kind of educational opportunity. Approximately 37% of those surveyed said they believed either classroom or e-learning training programs would be the most effective way to help them bolster their skills.

Meanwhile, specifically on the security front, developers are being left to twist in the wind by their employers. We've established the lack of security content in the typical software engineer's computer-science collegiate learning. For most developers, enlightenment doesn't come easily once

What do you think is the most effective way to continue your education/ gain new skills?



Developers: Does your organization provide you with adequate training in application security?

Security Staff: Does your organization invest enough in training developers in application security?

they hit the employment pool, either. Just about seven in 10 developers today complain that their organizations simply do not provide them with enough training in application security for them to do their jobs well.

Our survey primarily focused on developer and operation populations, but when we questioned a select group of security staffers in the DevSecOps world to supplement our research, they were even more pessimistic about how well their organizations were instilling appsec knowledge in the engineering department. Over 85% of security experts reported their organizations' inadequacy on this front.

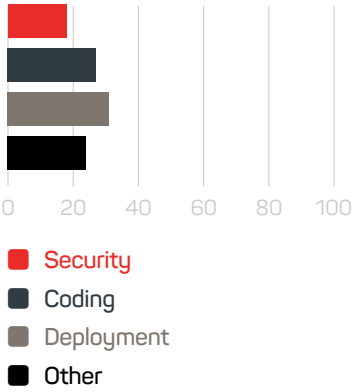
"I think as an industry, we've got to pull our socks up," says Daniel Cuthbert, a longtime security researcher, expert in penetration testing and COO at security consultancy SensePost. Continuing education opportunities for DevSecOps are still few and far between, he adds.

"In researching sec DevOps courses, there just isn't much out there. And a lot of the developer training courses we've seen are still teaching methods from a decade ago–waterfall security, pen testing at the end," Cuthbert says. "[They're] expecting developers to be hackers, and they're not. Developers build stuff. They don't want to be hackers."

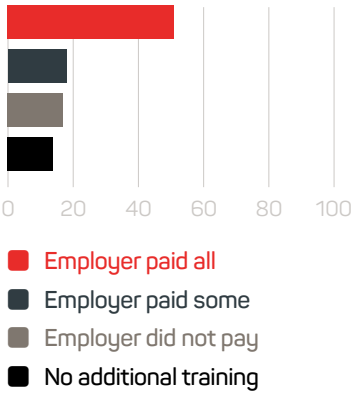
The immaturity of the DevSecOps training market offers a bit of a chicken-and-egg thinking exercise: Is participation low in this training because the content is stale, or is the content stale because there's still not enough participation to support better offerings?

For example, the SANS Institute is recognized as one of the premier providers of information security training on the

What skills have you acquired though eLearning



If you've received additional training since joining the workforce, did your employer pay for it?



market. It offers a five-day course on how to securely develop software, but it struggles to fill seats in the classroom.

"It does not sell," says Lance Spitzner, research and community director for SANS Securing the Human program. "We were asking, 'Why doesn't this class sell?' We think it is because no company is willing to give up a developer for five days. So the problem you have is most of that awareness training and secure code training for developers has to be online and measured in hours, not days."

That would likely account for why our survey respondents heavily favor e-learning over classroom training–by a three-to-one margin–as the most valued form of continuing education. According to the survey, over 80% of respondents had acquired security, coding or deployment skills through e-learning.

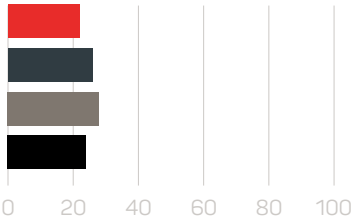
Another big sticking point that could be holding back mass acquisition of new DevSecOps skills is the cost of the courses themselves.

"If you look at industry trainings, there are a number of good courses out there, but the problem is that they're expensive," says Olsen, explaining that a SANS class such as the one Spitzner mentioned will run close to $6,000, while training courses at conferences such as Black Hat will run over $3,000 for a two-day class. "There's very little financial aid structure, and that locks out the smaller businesses and lower-income students who are going to try and do this on their own."

As things stand, only about half of respondents said they were able to get their employers to fully foot the bill for training they'd received since joining the workforce.

CISOs Take Note: What DevOps Orgs Need From Security

Which skills/knowledge do you wish your colleagues in the security organization would work to improve?



Establishing effective security training for developers and operations is but one facet of the process of skilling up a team to securely deliver software at DevOps speeds. In order to fully embrace DevSecOps principles, security personnel will need to upgrade their own skills to prepare them for some pretty radical shifts in how they do their jobs every day.

DevSecOps will require security practitioners to re-evaluate tooling and processes to fit better into the continuous delivery process. And that will require security personnel to bone up on their baseline knowledge of how developers operate and the constraints these software engineers face. Security people must meet the development team halfway on bridging the knowledge gap.

"I think it's all too easy for us as security people to say, 'Developers are stupid and they're doing it wrong,'" Cuthbert says. "Actually, we can learn a lot from how they're doing it. We've got to evolve as well."

This means that countless penetration tests with no clear action items for developers or scans that aren't streamlined into continuous delivery tools simply won't fly in a DevSecOps model.

"We're still doing it the same way we did in 2000, and that's not cool anymore," he says. "It's not good in a CI/DevOps environment — it slows things down."

Velocity is key. Any training or wisdom the security team can acquire to help it learn how to adjust their practices, their architecture and their toolchain to facilitate speed of delivery is going to reap serious benefits.

"It's about getting out of the mode of being the 'CS-nO'–the guy who says 'no' to everything and getting into the mode of helping developers and operations teams get their stuff done quicker," Feiertag says. "That's, I think, the most important thing for security folks as a whole to really internalize. Because frankly, if you move faster, you can be more secure. You just have to iterate it on your security just as you are on your software."

Paying Down Personnel Debt

"Some organizations are starting to develop what they call a 'security developer champion.' So all of your developers go through some basic developer training, security training and then you have a leader in each group that goes to super-security developer training."

— Lance Spitzner
Research and Community director, SANS Securing the Human program

A simple solution for the kind of personnel debt that's accruing doesn't exist. Organizations are rushing headlong into DevSecOps, and the market has only so many experts available with solid cross-training in DevOps and security principles. It's going to take sustained effort across the entire industry to improve that. But as organizations begin to face the immediate reality of some of the deficiencies uncovered by our skills survey, there are some first steps they can take to improve their situations.

Invest time and money for continuous education

First and foremost, continuous education is a must for continuous and secure delivery of software. Organizations that want to move fast and minimize risks need to train their staffs accordingly, particularly developers who are being called on to enact appsec strategies at the ground level. If your organization struggles to justify sending developers away for extended training classes, one suggestion might be to stud the developer corps with a few highly trained appsec experts who can help train their colleagues on the job.

Embed security in every training opportunity

Security principles are difficult to get to stick within the engineering department because they're rarely add-on skills that can be learned in a couple of days.

"It's about creating the mindset where the application developer knows that whenever they add a functionality, they are probably increasing the attack surface."

— Stefano Zanero
IT consultant and associate professor, Politecnico di Milano

"It's not just installing it and showing some basic demonstration," RIT's Sanders says. "There's got to be a strong, fundamental understanding of security architecture and how to deploy things in a way that isn't going to break both from a scalability perspective and from a future risk and attack perspective. It's a difficult combination to achieve."

This is why security experts believe that security classes are good, but meshing security principles within every education opportunity is even better.

"It needs to be embedded in the continuous professional development content," Zanero says. "We are beginning to see professional societies that are starting to structure it that way. It's about creating the mindset where application developers know that whenever they add a functionality, they are probably increasing the attack surface."

Ensure applicability

Finally, whether training is for developers, ops or security personnel, it should be targeted and applicable to the specific role.

"If you're taking the opportunity to train your broader engineering organization on security, you want it to be deeply applicable," says Zane Lackey, CSO at Signal Sciences. "They're not going to leave as complete security experts, but instead they should have a deep enough understanding that they can reach out to their development lead, DevOps manager or security engineers to ask the right questions when they need to."

Appendix

The "2017 DevSecOps Global Skills Survey" was conducted by DevOps.com and sponsored by Veracode. The survey was conducted online in May and June 2017. Participants came from organizations of varying sizes and based around the world. They were invited to participate via social media and email invites sent to DevOps.com's qualified database of IT professionals.

397 Total Respondents

How many employees does your organization have?

- 1-99
- 100-499
- 500-999
- 1000-4999
- 5000-9999
- 10000+

Which of the following best describes the principal industry of your organization?

- Telecom, Technology, Internet & Electronics
- Finance & Financial Services
- Healthcare / Pharmaceuticals
- Business Support & Logistics
- Government
- Other

In what country do you work?

- N. America
- Europe
- Asia
- Other

In what IT specialty do you primarily focus within your org?

- Development
- Operations
- Security
- QA
- Support
- Other
- Non-IT role

Which best describes your role at your organization?

- Individual Contributor
- Manage one team
- Manage teams
- Other

How long have you been in the workforce?

- 10+ years
- 5-10 years
- 3-5 years
- 1-3 years
- < 1 year

Highest level of education completed?

- Doctorate
- Masters
- Bachelor
- Associate
- Some college
- High school

In what area of study did you earn your degree?

- Computer Science
- Liberal arts
- IT-specific
- Other