Training: the secret to ongoing compliance

by Sammy Migues, Director, Knowledge Management and Training

July 24, 2007

Ongoing compliance requires ongoing training

Hundreds of thousands of companies around the world have collectively spent billions of dollars in response to the security- and privacy-related compliance mandates of the past 10 years. They have all increased staffing, upgraded physical security, deployed technology point solutions, rolled out new processes and digested hundreds of vulnerability and application scanner reports.

So, why are data breaches and other security failures still a common occurrence? Inadequate technical training that provides only basic awareness, a hallmark of a reactive security approach, is one of the simple answers. The need for security awareness training seems well understood, even if most organizations fail to follow through.

While many compliance drivers use the word “awareness,” however, the intent is that individuals are able to perform their job adequately with respect to protecting systems and data.

In fact, ongoing data breaches clearly show that reactive training that only conveys awareness is insufficient to meet organizational needs.

The ongoing evolution in security attacks, application development technologies, security software, testing automation, and especially in compliance requirements, necessitates ongoing training just to enable architects, developers, testers and IT security staff to continue to be effective. This training must be tailored to the audience—architecture risk analysis training for architects, defensive programming training for developers, risk-based and white-box security testing for testers.

The current Payment Card Industry (PCI) Data Security Standard (DSS) provides a good example of the increasing need for technical execution training. The PCI DSS requires:

• a firewall with a good default-deny configuration;
• removing vendor-supplied passwords;
• using anti-virus tools and intrusion detection;
• setting logical access controls;
• rolling out security policy and;
• establishing good physical access controls.

Almost everyone now expects their IT security staff to be able to deal with these basic issues, usually requiring no more additional support than vendor-supplied training on a particular technology. However, PCI also requires

• good use of encryption in several areas;
• a secure software development lifecycle;
• code review;
• effective vulnerability scanning; and
• penetration testing of systems and applications.

Very few organizations can afford to stop their IT, software, or data security activities for days or weeks at a time and send everyone to training. To compound this problem, generic commercial training likely will not help your practitioners correctly perform critical compliance activities that must be carefully tuned to the organization’s needs.

In our experience, and as easily found in the popular press, even the most modern IT security technologies cannot prevent a flawed application from divulging sensitive information. Software security must improve and ongoing technical training that reliably increases practitioner skill is a

1 In April 2007, AMR Research reported that spending on SOX compliance will rise slightly in 2008 to reach $6.2 billion, resulting in a cumulative $32.3 billion spent on SOX compliance alone. The bulk of that investment (almost $24 billion) has been in people and consulting services, with only $8.6 billion having been spent on technology.

2 Other “simple” answers include the rapid introduction of new software development technologies, the constantly changing threat model, and security tools and technologies that simply do not work as advertised. However, proactive security that includes good training allows organizations to work around these complexities.

3 In early 2007, a CompTIA survey showed that while human error accounted for 60% of information security breaches (up from 47% in 2005), only 29% of organizations required security training for IT staff. In Cigital’s experience, the percentage of organizations providing security training for employees involved in the software development lifecycle is far smaller than even 29%.
required foundational building block. It is possible to make quick progress with a good strategy and a partner with good software security experience.

Making Good Training Material

When you’re thinking of making or commissioning some technical training, first consider these three fundamentals:

- “This training is appropriate for people who...”
- “In this training, you will learn how to...”
- “After this training, you will be able to...”

You may need a formal performance needs assessment to get requirements for technical training. This process must define the gaps between desired and actual performance and help determine root causes. Given this information, it is possible to define basic training needs. Include the appropriate internal and external technical experts in this process to ensure the training is skill-level appropriate and actually addresses the documented deficiencies. You should be able to tell the students something useful about the course, such as, “This course shows developers how to use white lists for data input validation in web applications. Doing this correctly will help the company meet internal security and external regulatory compliance requirements.”

This makes it clear the training is not just a check-the-box exercise; the students know why they are there and how their efforts are going to really help. Continually reinforcing why the training produces practitioners who are more business-risk aware. With the right kind of positioning and reinforcement, students later are inclined to ask, “How does this affect the business?” and be more likely to ask someone rather than just putting some technology together. tricky).

Lack of time or expertise invested produces poor training materials that are simply about the topic, not on how to do the topic.

Organizations should budget about 100 minutes per technical information slide to create useful material focused on imparting a single important idea in a memorable fashion. This includes sufficient time for creating instructor and student notes. This 100-minute block also allows for internal review, discussion, and training and practice for the first instructor.

One hundred minutes per slide may seem excessive, but if you’re spending less than three work-days to plan, draft, and complete one hour (about 15-20 information slides) of technical training telling someone how to do something, your efforts are probably insufficient.

- Seize every opportunity to customize the training to a specific group’s needs, mentioning specific policies, prescriptive guidance and references.
- Remove every group of words, bullets, or slides that can be replaced with a diagram or picture.
- Decorate each picture appropriately, without having it so busy that it becomes an unreadable.
- Animate each picture whenever necessary to show how and when things actually happen.
- Create pictures students can reuse in their jobs.

Poor slide, dense, multi-topic, confusing, visually defunct

What Are They Looking For?

- Core are Core Concepts
  - Course is a Course Topic
  - Course is a Course Topic

Single idea slide with a related visual for interest

Anatomy of a metric (fully specified)

- Name & Description
- Purpose/Objective
- Data Sources
- Formula
- Units of Measure
- Thresholds
- Visualization Methods

Always include exercises that get students thinking about practical application. Also, include quizzes that reinforce the training’s main points. Depending on the complexity of the material, it may be wise to follow-up with a second quiz some weeks or months later. Be conscientious
in grading quizzes and giving students honest feedback.

The long-term benefits derived from putting the required time and skill into building good training materials will far exceed the initial investment. Employees will benefit from the increase in skill and the organization will benefit from the increase in security and, thereby, compliance.

Executing on Good Training

Companies must find the training styles, and the experienced instructors, that work for their people in their environment. Even allowing for organizational diversity, however, there are a few universal items to demand from trainers:

- **Be as formal in your presentation method as you need to and then just a touch more.**
- **Stick to a schedule.**
  Don’t wait for that last straggler and penalize everyone who was punctual. Class Management is part of the instructor’s job.
- **Use eLearning (computer-based training, etc.) for awareness training and basic skills for the masses.**
  It is very important, however, to use instructor-led training (ILT) for teaching important execution skills to your practitioners.
- **Ensure the instructor can actually teach the material in the time allotted.**
  Ban all gadget distractions. If the last 20% of the material has to be rushed students feel cheated.
- **Give people sufficient breaks to avoid other rule violations.**
  Most people can concentrate only for about 90 minutes at a time. Partition material with this in mind. Provide access to snacks, beverages, restrooms and network connections for breaks.

The instructor must know more than what’s in the training materials.

If the instructor cannot go off-script as needed to enable comprehension, you may need a different person, whether an employee or a partner.

Prompt students to show they are “getting it”

When presenting technical training material always ask some open-ended questions. Prompt students to use their own words to show their thinking.

If an organization truly cares about the quality and effectiveness of its training, as well as the behavior it seeks, it will show in the material and in the delivery. This energy is contagious. Training allows employees to stretch themselves in new and challenging ways.

Follow-Through for Compliance Success

Pitch training reinforcement messages at the right level

To get people to learn the theme, match the message to the audience. Tell people who work with software bugs about bugs, then their bosses about trends in bugs, and the next level about trends in application quality, and their bosses about trends in the application portfolio, and so on.

Companies must to work diligently after training to eliminate any gaps between what the students are doing and what the organization needs them to do.

With respect to software and data security compliance, this will be a moving target and the company’s training program or partner must keep up. Continue to remind employees of what they already know and explain to them what you want them to do that is extra or different.

Tracking performance is critical to success.

After taking the time and expense to increase employee skills to make ongoing compliance possible, make the corresponding activities part of the metrics that someone tracks. After teaching a roomful of testers how to do inside-out white-box security testing, keep track of the software flaws caught as part of this process, along with relevant trends.

A similar useful metric might show which code bases are exhibiting the most problems and how that tracks back to the composition, training, and automation support for the various development teams. If the organization can discover which teams are routinely making similar errors due to, say, having a broken unit testing process or even a misunderstanding of the compliance requirements, everyone wins.
Find the stars from your training sessions and groom them appropriately.
They may be the next crop of team leaders or managers. Evangelize training by having one or more of those individuals improve the course material or even teach the next class after going through an instructor certification process.

Always follow up with instructors as well.
Do post mortem reviews after each class to give constructive feedback. Ensure that every student completes a feedback form that gathers useful information, not whether they enjoyed the class.

Provide assessment for the investors.
It is not just the individual student that must get something out of the class. The people covering the costs likely expect specific accomplishments from the students, such as an effective ability to include white-box, risk-based security testing a part of the quality assurance process. Track these metrics and ensure everyone sees how the investment paid off.

Conclusion
There is often a clear path to getting employees to do the right thing. Explain clearly what is expected, make it part of the business process, and give them the proper training and tools. Ensure there is good alignment between what they are being asked to do and their individual goals. Then, track progress and make course corrections as necessary. Most organizations do this every day in the executive ranks, but the organization’s ability to get and remain compliant. Good planning, training, and follow-up will better ensure long-term success.

In Cigital’s experience across a variety of organizations, customizing training to include specific references to relevant policy, software prescriptive guidance, and additional internal and external resources is key to adoption and use. Cigital has used its wide-ranging experience to develop a mature software security course curriculum. We have also certified a cadre of instructors that can deliver our state-of-the-art software security training, as well as engage with organizations to extract key business objectives, security and compliance requirements, and existing skill sets to allow creation of a tailored education curriculum. Our ability to plan and deliver a long-term skills improvement program ensures that security and compliance needs are met on an ongoing basis.

About Cigital, Inc.
For over a decade Cigital has enabled some of the most well known companies in financial services, communications, insurance, hospitality, e-commerce — as well as government agencies—to resolve their mission-critical software business risks. Cigital clients are able to protect some of their most valuable assets: company information, customer data, shareholder value, and brand.

Cigital helps assure the reliable delivery and deployment of software that organizations build, buy, and integrate. Cigital’s services include:

- Enterprise Risk Management
  - Secure SDLC
  - Sensitive date protection
  - Portfolio risk analysis
  - Compliance software issues
- Software Security Assurance
  - Secure code review
  - Architectural risk analysis
  - Security testing
- Software Quality Assurance
- Training

The company is headquartered near Washington, D.C. with offices in Boston, New York, and Los Angeles.

Sammy Migues is the Director of Knowledge Management & Training at Cigital, Inc. Mr. Migues has a proven record of entrepreneurial innovation, intellectual capital development, practical business solutions, and performance optimization. He has extensive day-to-day experience in chief architect, chief technologist, and evangelist roles, working directly with customers, product management, and product development.