iapp

MUST-HAVE
Privacy Training Features for Your Team

ShanShan Pa, CIPP/E, CIPP/US, CIPM, Alibaba

A privacy program cannot be successful without training. There is a Chinese saying: "Those who want to get the job done must first sharpen their tools." An effective privacy training not only enables an organization's privacy initiatives, but also enhances an organization's overall operation in the areas of Privacy by Design and data protection-centric security practices.

What are the must-have features of an effective privacy training for your team?

It all starts with a "Why."

The worst thing you can do is to train for the sake of training, itself. Often, we jump immediately into the content of the training. After all, time is money, and training requires taking time away from people performing their daily jobs. However, not fully understanding the purpose and the motivation behind the training program will only waste more time and money later on in retraining. Therefore, an introduction to the "why" of a privacy training program is essential.

Examples can be real-world business cases or current events that are privacy related, so that people can easily relate it to themselves or their daily works. The passing of the GDPR or increase of audit focus on HIPAA compliance might not be as easy to digest for a person new to privacy as the story of a company that violates user consent by selling consumer data to third parties for profit, or that of data stolen by a hacker. When privacy is still a new concept, people need that extra context to grasp the idea of data protection.

> Knowing your audience is the golden rule for any presentation or sales pitch, as it is for a privacy training.

Knowing your audience is the golden rule for any presentation or sales pitch, as it is for a privacy training. Especially, privacy-related content cannot only focus on laws and regulations. If the attendees are from technical teams, then be more technical, or at least have the example cases relate to the technical area, such as explaining how creating a pop-up window to notify users about cookie use is part of notification and choice. Or how creating a new registration workflow in the backend for the website that collects children's information is done to comply with COPPA requirements.

Even if the audience is a room full of lawyers, do your best to bridge the gap between legal frameworks and business systems and operations. The training itself should translate the same content to different departments of an organization in different ways, while at the same time gluing them together with the same goal: the organization's commitments to privacy.

Nor should you think you can accomplish training in one class, once a year. Training must come in continuingly different formats depending on the size of the group, the type of training, and available budget. It's easy to say "You get what you pay for" when dealing with constraints, but each organization is different and targeted training needn't be expensive or overly time-consuming.

It might be hard to pull together a 50-person training class all at once, with many schedule conflicts and people needing to travel great distances for a big organization. It might be even harder to find an affordable professional training class for a small organization. Don't let cost, geographic locations or the scale of the teams be excuses. With technology today, we are offered many more options than ever before.

For example, the IAPP provides various resources for training, such as classes, online trainings, conferences, local KnowledgeNet meet-ups or books and webinars. Use Skype or FaceTime to bring satellite offices together. The key to make any training effective is frequent reinforcement. It doesn't matter what format of training you started with; continue to reinforce the material throughout the year. Maybe you can launch a monthly privacy newsletter email or a quarterly lunch-and-learn focusing on privacy best practices and privacy program progress. Maybe it’s just a poster in the watercooler area.

Keep carrying on. Not only it will raise overall awareness, but it will also become part of the company culture and practice.

And who says a privacy training cannot be fun? Be more interactive and collaborate, create group exercises or have it outdoors (PII scavenger hunt anyone? Somewhere safe please!). That way, people are more involved and willing to further explore on the topic. Have visuals and flowcharts for people who absorb visual information well, or watch a new movie with privacy themes and discuss it together. Every training is a knowledge transfer, and, with privacy, it is not only for the organization’s benefit. It will definitely benefit your colleagues’ personal lives as well.

Last, but not least, an important training feature that is often forgotten is the feedback step. At the end of every training, remember to take feedback from the audience and the instructor. Only then can you improve the program to make it more effective and tailored to your organization. How did the audience think the program related to their daily work? Does it make them more open to learning more about the topic or the opposite? The instructor can also provide feedback on the interaction or the reaction of the audience to the topic. Feedback is key for measurement; it shows how privacy is presented and perceived in the organization. Throughout time, organizations should notice the maturity level of the privacy practice improving.

If not, perhaps the training isn’t effective!

At its core, training is a learning experience for every organization as it looks to add value to its business and its people. A thousand mile journey begins with a first step.