iapp

How Privacy Awareness **BUILDS TRUST**

Ben Siegel, CIPM, Privacy Ref

Trust is an important part of business. One of the benefits smaller organizations reap better than any global conglomerate is the trust of their customers. When you buy something from a local store, you know who you are buying it from and any problems that arise are expected to be handled locally, not by a customer service center that is possibly half way around the world. Many consumers shop at local establishments for just that reason; they believe they can trust that business more than others.

An example is buying something, let's say a coffee maker, online as opposed to the local store. In the case of the prior, if there is a problem where our coffee maker doesn't work correctly or arrives broken, we must go through a whole process of calling customer service, sending the appliance back, waiting for a new one, or potentially not getting any refund at all because somehow the warranty was voided. In the latter example, you still must get in contact with the store, but you can physically drive there, speak with someone in person, and get an immediate response.

Who would you trust more, someone you know or someone you are working with on the phone? Privacy pros can draw from this trustworthy local business model when developing privacy awareness within their organization.

---

1. Train toward awareness

Privacy training programs have the goal of teaching your employees how to process, protect and handle data. This is especially important because your employees are the ones handling a multitude of tasks each day that utilize personal information, including during privacy-related events and incidents.

A privacy-aware staff may stop an incident before it happens. They can catch suspicious emails, report strange activities on your servers, identify and report suspicious activity, or simply make sure to double check the recipient of an email containing sensitive information. These activities create integrity within your security and privacy programs and serve to build trust with customers.

Through your privacy notice and day-to-day interactions with your customers, your employees can share their knowledge of your privacy practices, allowing customers to share their personal information with confidence and trust.

2. Privacy for the people

The strength of your privacy program will not just show in your lack of negative events, but also in day-to-day interactions with customers.

As consumers become more privacy savvy, they will have questions for your employees about how their data is used. Employees now have an opportunity to win over that customer and possibly lock in their future business. One of the easiest examples where you can see this is in a rewards card program.

> **The strength of your privacy program will not just show in your lack of negative events, but also in day-to-day interactions with customers.**

Retailers often have a rewards program where customers use a card at the checkout for discounts or points in exchange for allowing that organization to track their purchases. Customers may ask what information is gathered or how it is used. When this happens, if your employees are unsure, the customer may interpret this as something being hidden from them, or incompetence, hurting your business. On the flipside, if your employees can answer the question succinctly, they will lay the foundation for a strong trust-based relationship with that customer.

Consumers will always question the value of allowing access to their data, but if you are

providing value in exchange for that data, without seeming shady or disingenuous, you will have a large loyal base of loyalty or rewards card holders. Remember that the difference here is simple transparency and openness with customers. Informed employees who are privacy aware can build that trust for you by simply doing their job and helping customers.

3. Taking the bad with the good

You will not always have the leisure of addressing privacy concerns in a calm environment. You will have incidents or even breaches of your company's privacy program that require you to respond swiftly. Just as you would be open about your organization's privacy policy with the rewards program, you need to be open and communicate the situation here. Many companies that fail to communicate about an incident fall victim to the "Streisand Effect", where the more you try to hide or ignore something, the more people will look for and find it. When you discover a breach, or any negative incident deserving of public comment, you want to be transparent about your actions.

If your company has confirmed a breach and decides to execute your breach response plan, you can take the opportunity make the public aware of your privacy practices. Make your customers aware of how you are following up. Let them know if and when you bring in third parties to investigate. Let them know how you plan to respond to potential threats moving forward. Let them know what other protections and practices you already have in place.

If there are questions about customers protecting themselves from fraud, be sure to instruct them on how they can protect themselves, or make them aware of services like credit monitoring you are offering in response to the breach. Providing this information to customers will build trust with them, maintaining that relationship, but also show responsibility to potential new customers.

It is very important to take responsibility for missteps in an incident. If there was a hack of your systems, you are a victim of a crime, but that also means there was some vulnerability. Facing the facts, owning them, and setting the path forward to improvement will show responsibility to consumers. Trying to hide the truth or shift blame can result in blowback from consumers. A negative reaction to this kind of response could mean a loss of customers, a dip in stock price for publicly traded companies, or a shakeup at the executive level to appease public outcry. All of this can happen as a result of a loss of trust.

4. Championing privacy

Privacy awareness is a tool that can be used to establish trust in the ways discussed above, but there is also another way to build trust. We often champion outstanding achievement in our businesses with easily identifiable metrics. Sales people often receive accolades for milestones, or customer service reps for outstanding service, but how do you champion privacy achievements?

Look for evidence of your employees developing consumer trust and reward it. This should be a key objective of your privacy program: privacy victories, not simply a lack of privacy failures.

When privacy awareness campaigns are utilized correctly, you will see increased customer loyalty and other benefits. When they're not, you open your organization up to loss of trust, loss of revenue, and potentially much worse.

FOR MORE PRIVACY AWARENESS IDEAS

check out the Employee Awareness and Education page in the IAPP Resource Center.