How to Foster Good Data Privacy Culture Now

By Larry Samilow,
Co-Founder and Managing Partner
Verve Group Consulting

With compliance with the California Consumer Privacy Act (CCPA) and other data privacy laws top of mind for businesses and the consumers who support them, now is an ideal moment for organizations of all sizes to focus a bit more effort toward enhancing good data privacy culture.

Why push for this right now? Customers care about data privacy, legislators are looking into it, and businesses are finding that good data privacy culture not only limits liability but can actually improve customer confidence and loyalty. A Pew survey revealed that 90% of respondents prefer to control the personal information about them that is available and being used by businesses. In the United States, politicians increasingly are seeking ways to protect online privacy through lawmaking.

The Business Case for Good Data Privacy Culture

Data privacy, according to an IBM survey, has joined customer relationships and workforce skills as one of the top three competitive advantages. Meanwhile, the average cost of a data breach is $3.9 million. Disregarding data privacy tends to be an expensive mistake.

> ***There is a business advantage in developing privacy policies, procedures and training materials in easy-to-understand language. "If we translate legal and regulatory requirements that our employees must follow into everyday language and in a format that is easy to read, people are more likely to read them," observes Blanche Stovall, JD, CIPP/US, CIPP/E, CIPM. "If people can read and understand these requirements, they are more likely to follow them," Stovall says.***

The bottom line? Good data privacy culture boosts customer confidence and loyalty. Fostering that culture is not so much a spend anymore as it is an investment—and an important one.

How to Achieve that Behavior Modification

Good data privacy culture consists of more than just information technology and Cybersecurity elements. Sound internal policies and procedures, along with appropriate training, also make up an important part of the mix, so much so that California actually included training requirements in its proposed regulations implementing its consumer privacy law.

While corporate codes of conduct might touch on privacy, their concomitant policies and procedures may need an update in light of this change in attitude toward, and regulation of, data privacy. Similarly, training may need a refresh to reflect more current approaches to data privacy.

Make Materials Accessible

One need only browse through the definitions section of any given data privacy law to realize that becoming mired in legalese can happen all too quickly. Consider, for instance, what exactly a "record" is. Is it on paper? Digital only? In handwritten employee to-do lists? Then contemplate varied meanings of "personal information" and all of its subsets—highly sensitive information, financial information, data on children of various ages, and so on. It can be easy to lose the overall message—protect private information and don't collect it unless it is really necessary for a business purpose—in a mélange of overlapping and varied requirements.

Effective employee policies and training materials have their foundations in straightforward and understandable language and guidance.

> ***Customers, employees, and third-party vendors appreciate materials that are not full of legalese. "Ultimately, customers want to know how their personal information is collected, used and shared, and what they can do to maintain some level of control over their data," says Stovall. "Employees want to know what they can and cannot do with personal data, and third-party vendors want to know what their obligations are in relation to their business customers."***

Behavior modification, especially where long engrained practices are involved, isn't easy. The tone from the top of an organization of course plays a part, but an enterprise is going to need buy-in at all levels to achieve meaningful and lasting change. Businesses have an opportunity to foster an ongoing commitment to protecting data privacy through the communications, training, policies, and procedures that address it. A similar transparent and easy-to-understand approach to customer-facing statements also helps.

A Phased Approach for a Reasonable Budget

Simply throwing money at the problem—"we need to do something on data privacy"—isn't going to create a good data privacy culture. Creating or revising sound employee policies and training materials can be done in phases and reinforced with supportive communications to create a lasting, and real, commitment to data privacy.