SOUTH CAROLINA SBDC

CONSULTING EDUCATION RESOURCES

NEWS

A PUBLICATION OF THE SC SMALL BUSINESS DEVELOPMENT CENTERS

Data Privacy and the Future of Business: How Businesses Can Put Privacy First

With the global big data market set to be worth nearly $235 billion by 2026, to say that data is now core to business success today would be a massive understatement. From tweaking shipping strategies to delivering more relevant advertising campaigns to customers, businesses are constantly looking for ways to make more data-driven decisions. But with this access to consumer data comes great responsibility. And unfortunately, in many consumers' eyes companies are not doing all they can to make sure that their data is being used securely and with the highest privacy standards in mind.

According to the Pew Research Center, 79% of U.S. adults report being concerned about the way their data is being used by companies. Respecting consumers' privacy is a smart strategy for inspiring trust and enhancing reputation and growth in your business. Be open and honest about how you collect, use, and share consumers' personal information. Think about how the consumer may expect their data to be used and design settings to protect their information by default. Communicate clearly and concisely to the public what privacy means to your organization and the steps you take to achieve and maintain privacy.

Conduct an assessment

Conduct an assessment of your data collection practices. Whether you operate locally, nationally, or globally, understand which privacy laws and regulations apply to your business. Follow reasonable security measures to keep individuals' personal information safe from inappropriate and unauthorized access and make sure the personal data you collect is processed in a fair manner and only collected for relevant and legitimate purposes.

Prioritize Third-Party Cybersecurity

Don't forget to maintain oversight of partners and vendors as well. If someone provides services on your behalf, you are also responsible for how they collect and use your consumers' personal information. And as this year's slew of supply chain attacks -- most notably the Kaseya and Accellion breaches -- have shown, third-party breaches can be just as hard-hitting as if your company was attacked directly. Therefore, companies need to have a rigorous checklist in place to ensure that their partners are taking cybersecurity and data privacy as seriously as your business is. Here are a few questions you should ask to get started:

- Does your company have written business continuity/disaster recovery plans? Are these plans tested on a periodic basis?
- Does your company hire an external audit firm to perform a compliance review of your operational controls?
- Does your company have a pre-employment screening policy for employees and contractors?
- Are files and records reviewed, retained and purged in accordance with legal requirements, contractual obligations, and service level agreements?

Adopt a privacy framework

Knowing the risks that your company's data faces is pivotal to making sure it is safely maintained and used. However, only 57 percent of businesses conducted a data security risk assessment in 2020. Researching and adopting a privacy framework can help you manage risk and create a culture of privacy in your organization by building privacy into your business. Granted, there are many different types of frameworks and some may work better for some companies than others. However, the following resources can help organizations get a sense of where to get started: NIST Privacy Framework, AICPA Privacy Management Framework, ISO/IEC 27701 - International Standard for Privacy Information Management.

Educate employees

Ongoing training and awareness campaigns for employees are a must for businesses today especially as the digital world becomes more and more driven by remote work. Unfortunately, many businesses are coming up short in terms of their training and awareness efforts. For example, 44 percent of organizations provided no cybersecurity training geared towards remote work for their employees.

Data privacy success hinges on a business's ability to create a culture that prioritizes privacy within their organization. And educating your employees about their role and your organization's obligations to protecting personal information is central to establishing this type of environment. Look to educate employees on your company's privacy policy and teach new employees about their role in your privacy culture during the onboarding process. Businesses can then begin to build on these fundamentals by setting up ongoing training and awareness sessions, establishing fireside chats with leadership around cybersecurity, and building toolkits for employees to refer to on a daily basis.

2021 was yet another watershed year in terms of business data use. And 2022 is likely to be another. Therefore, it is imperative that businesses put their best foot forward when it comes to data privacy, and these few steps can help them make significant strides in developing better privacy habits.

CONSULTING
EDUCATION
RESOURCES
SC SBDC